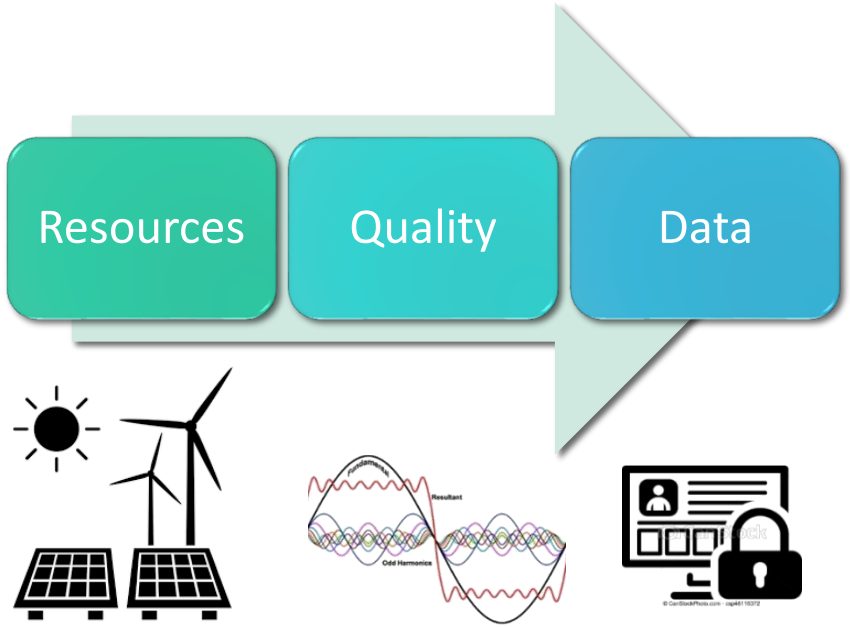
Europäischer Fonds für regionale Entwicklung (EFRE)
Der Oberrhein wächst zusammen mit jedem Projekt

WP7- Data security in smart grids

IRIMAS Institute, University of Haute Alsace
Bushra CANAAN
Djaffar Ould Abdeslam

Energy Security :



Moving from Geopolitics security

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

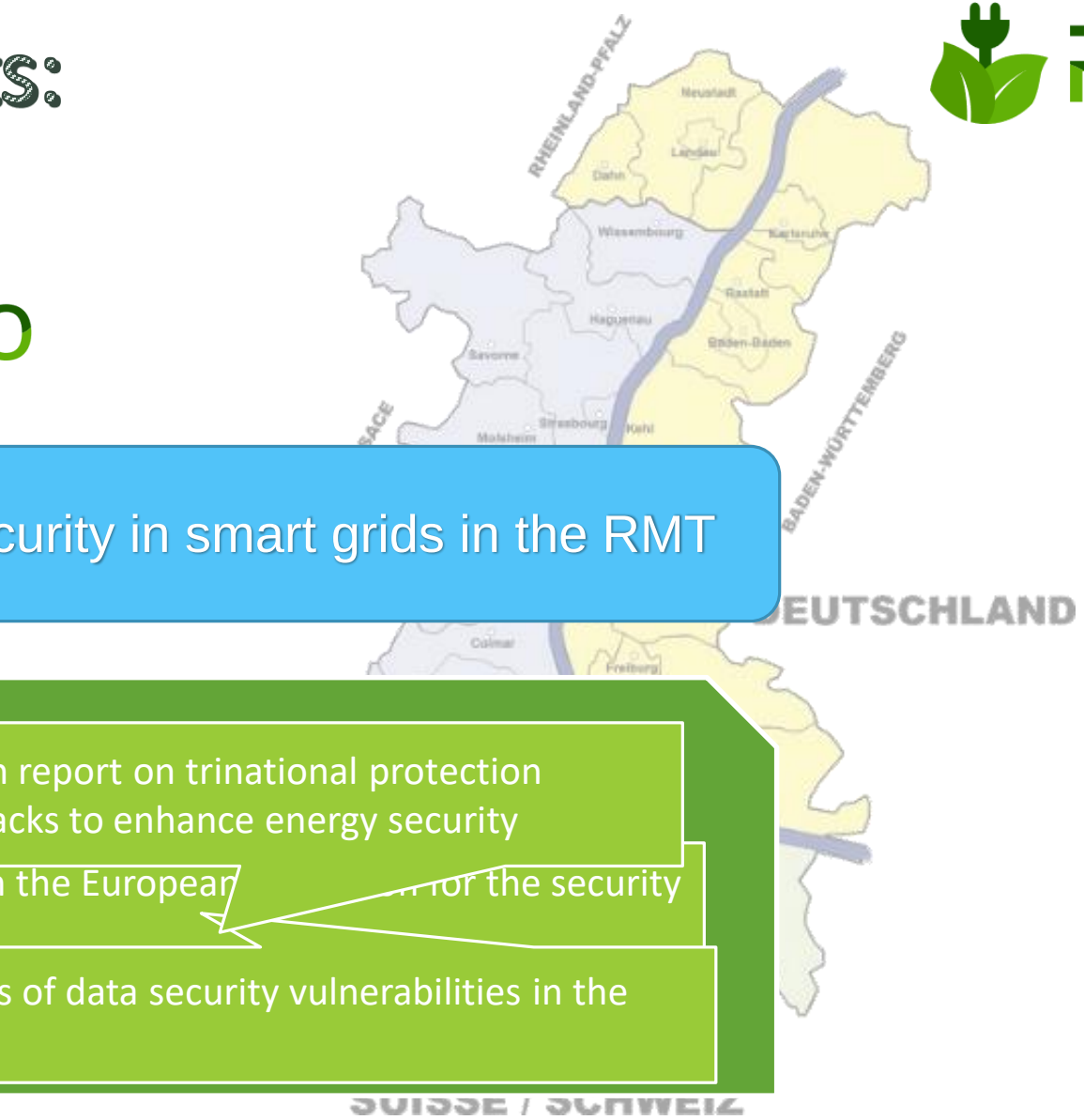
- Distributed energy resources (DERs) have changed the way the energy grid has worked for the past 150 years.
- The intermittent nature of Distributed Energy Resources must be counteracted with highly scalable data analytics that allow us to detect, predict and prevent any issues.
- Governing and sharing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

Cross-boarder security :

- Cross-border regions serve as testing grounds for European integration.
- the economic rationale for cross-border collaboration is compelling and goes even beyond the economic rewards to include creating long-term relationships to driving innovation.
- Boosts market confidence and provides investors with safer trading conditions.
- It creates a more dynamic, efficient, and integrated internal energy market by building equal competitive conditions field between Member States and encouraging the harmonization of national legislative and policy approaches.
- Hence it might help the Energy Union fulfilling its goals more effectively while also improving the energy system's security and resilience.

WP Outputs:

RES-TMO



WP7- Data security in smart grids in the RMT

- Recommendation report on trinational protection against cyber attacks to enhance energy security
- Detailed report on the European [illegible] for the security of energy data
- Predictive models of data security vulnerabilities in the TMO

7.1.1 Detailed report on the European legislation for the security of energy data

Provide a brief review on the latest legislations, measures and initiatives adopted by the EU in terms of cyber security. With a special focus on **smart grids** to support electricity security during a period of rising digitalisation and decentralisation (Distributed Resources Control and meters).

Utilities and other infrastructure have become increasingly attractive targets for bad actors, whether for financial or political gain. Attempts to breach systems grow, especially for **systems that control vital infrastructure such as the electric grid**.

The European Union (EU) boasts one of the world's most stable electricity systems and a high level of energy security, thanks to its oil and gas reserves. However, a number of existing and emerging phenomena, particularly in the electrical industry, offer new threats to energy supply security.

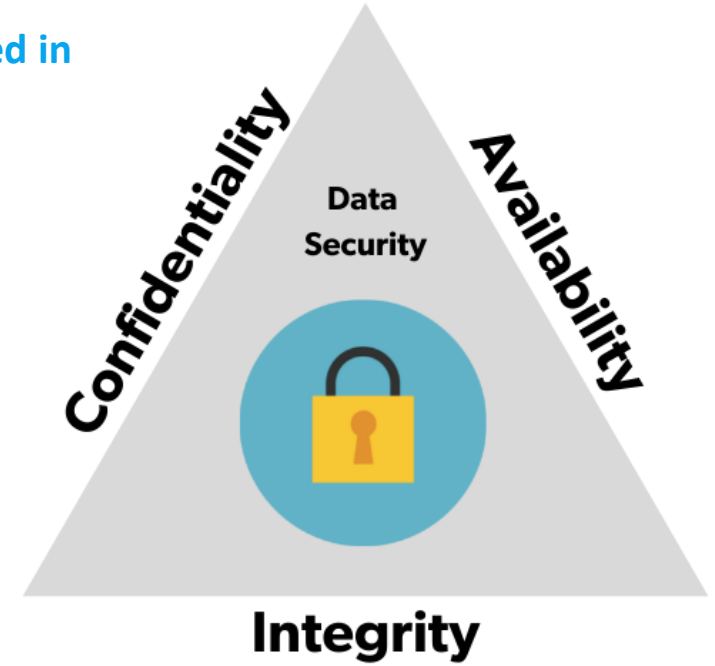
A **new regulatory framework is necessary** to ensure the most effective type and level of incentives to stimulate the investments required by the transition towards Smart Grids, while ensuring a level playing field in the sector

7.1.1 Detailed report on the European legislation for the security of energy data

How energy is different from any other industry in terms of cyber security?

what are difficulties that need to be addressed in the energy sector?

- Real-time requirements
- Cascading effects
- Combined legacy systems with new technologies



How could attacks effect the Energy system?

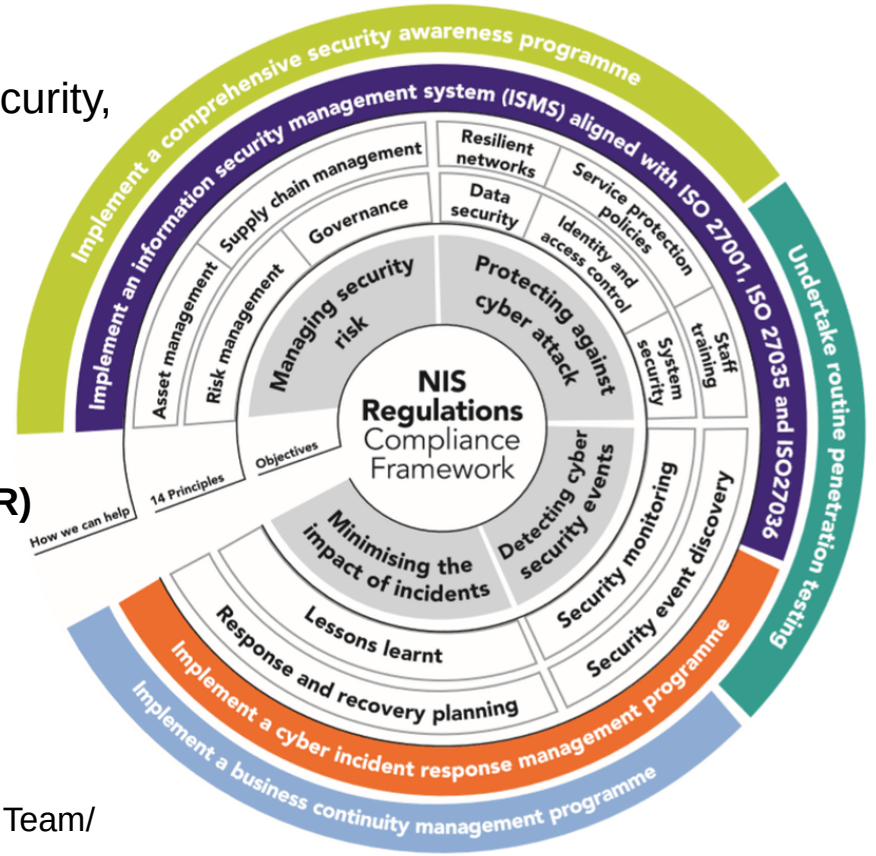
- Day-ahead market and
- Real-time market.

7.1.1 Detailed report on the European legislation for the security of energy data

NIS Directive

The first EU-wide legislation on cybersecurity,

- Improved cybersecurity capabilities at national level.
- Increased EU-level cooperation.
- Risk management and incident reporting obligations for operators of essential services and digital service providers.



General Data Protection Regulation (GDPR)

Improve the handling of cross-border Incident Response

Minimum set of capabilities

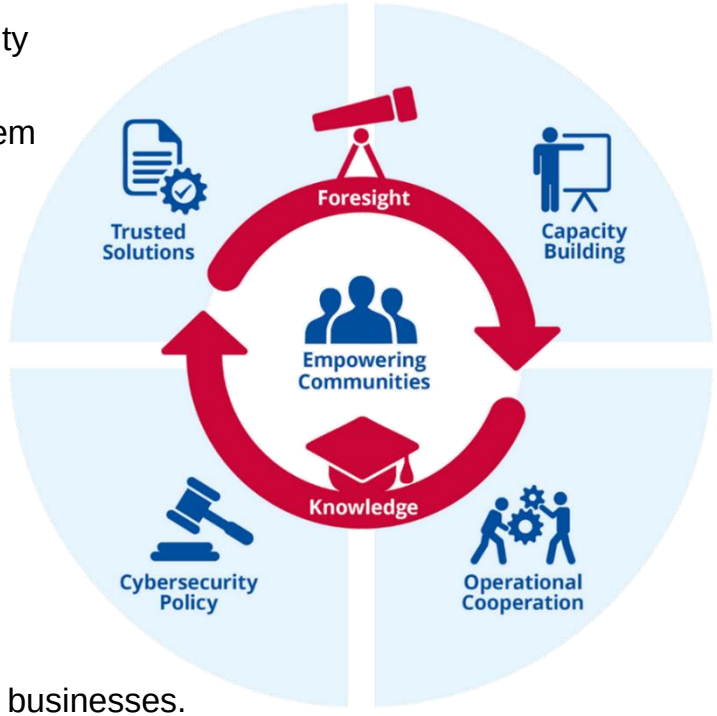
- national strategy,
- national competent authority/ies,
- national Computer Security Incident Response Team/ CSIRT

7.1.1 Detailed report on the European legislation for the security of energy data

The Cybersecurity Act

The European Agency for Network and Information Security ("ENISA")

European system of certification of the cybersecurity system for digital products and services



ENISA:

Market observatory' to analyse the trends of the cybersecurity market and then reflect that in the EU policy development in the ICT standardization

Involved in the EU Cybersecurity Blueprint.

EU cybersecurity strategy

Strengthening Europe's resilience against cyber threats

Ensuring reliable services and digital tools for citizens and businesses.

7.1.2 Report on the responses to the survey of electricity grid operators in the three regions

Stakeholder Cybersecurity Certification Group

RES-TMO

Information sharing can improve cyber resilience across the system, all stakeholders in the electrical sector should be encouraged to disclose information about vulnerabilities and actual incidents, to be honest about policies that have been enacted, and to share information and best practices at both the national and international levels.

In order to ensure the cyber resilience of the whole power value chain, policymakers, regulators, utilities, and equipment providers all play critical responsibilities.

Workshops discussions evoked key needs & requirements from these stakeholders as well as to validate the content of this report.

7.1.2 Report on the responses to the survey of electricity grid operators in the three regions

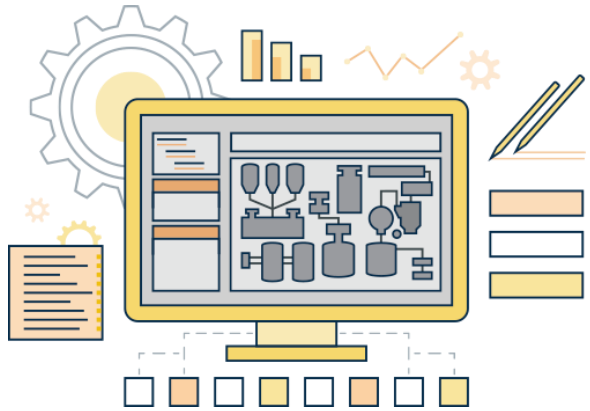
- Energy Citizen-based renewable energy, emergence of a local project: challenges and levers for action (Strasbourg 23/09/2019)
- Citizens as Prosumers: Legal Status, Rights, Involvement in the Energy Transition (07/10/2020)
- Regional energy resilience and decarbonization through decentralized RES: pathways, technologies, regulations, challenges (10/11/2020)
- Regional energy resilience via distributed RES and the role of smart grids: challenges and opportunities (cyber security) (04/05/2021)

Informal interviews and discussions with experts within the consortium

French distribution operators **Enedis**, transmission operators **Rte**

Challenges :
Smart and connected features (smart meters)
Data sharing strategy
The new role of DSO as Gestionnaire de reseau informatique.

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Publications:

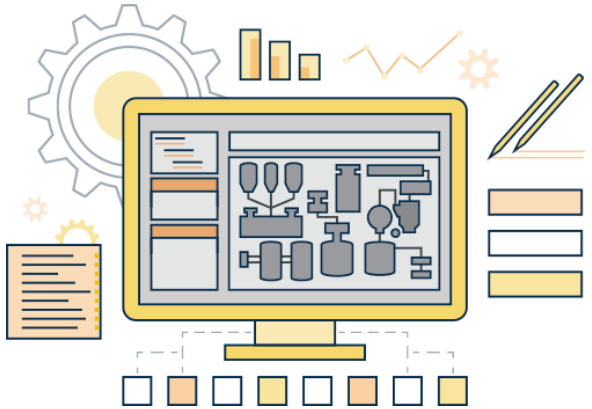
Journal paper: Microgrid cyber-security: Review and challenges toward resilience

Conference paper: Detecting Cyber-Physical-Attacks in AC microgrids using artificial neural networks

Book Chapter: A regional cross-border approach to the energy transition.

Accepted conference paper: Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Publications:

Journal paper: Microgrid cyber-security: Review and challenges toward resilience

- 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

Open Access | Feature Paper | Review

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.

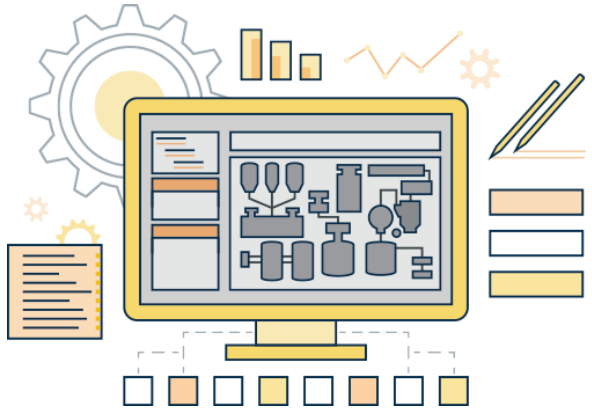
Appl. Sci. **2020**, *10*(16), 5649; https://doi.org/10.3390/app10165649

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)

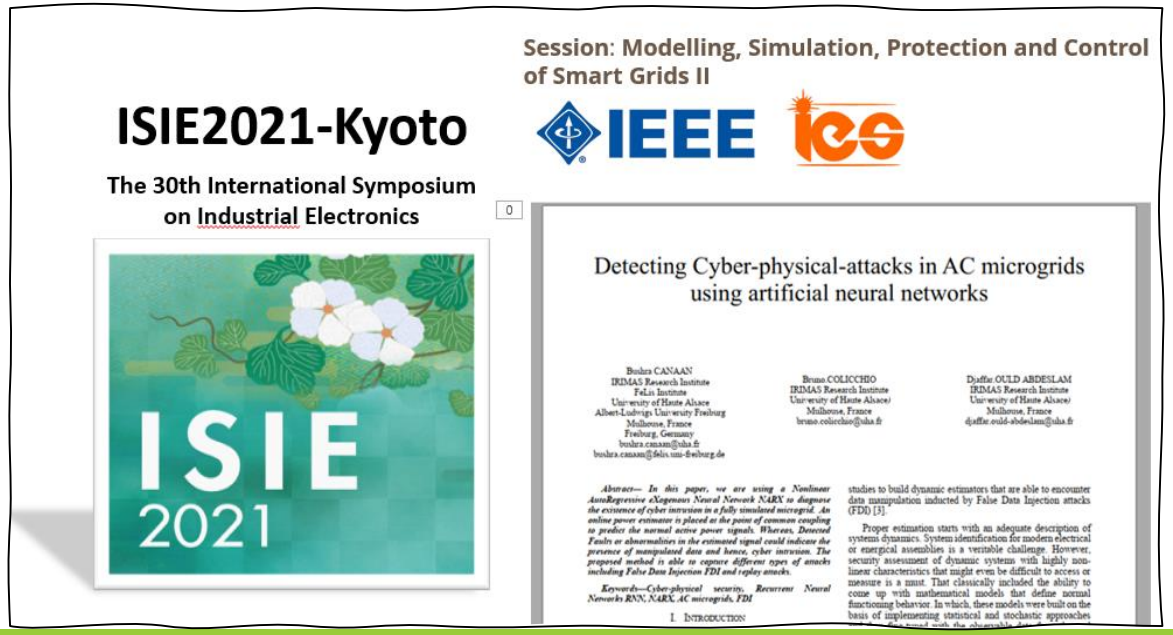
View Full-Text | Download PDF | Browse Figures | Cite This Paper

7.2 Predictive models of data security vulnerabilities in the TMO

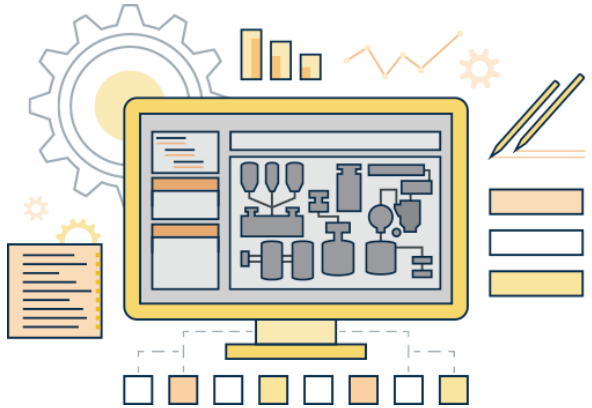


Publications:

Conference paper: Detecting Cyber-Physical-Attacks in AC microgrids using artificial neural networks



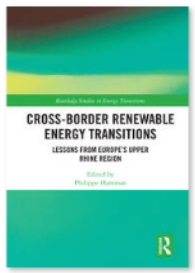
7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Publications:

Book Chapter: A regional cross-border approach to the energy transition.



Chapter

A regional cross-border approach to the energy transition

Political context and decarbonisation pathways, renewable energy potentials and two energy system models

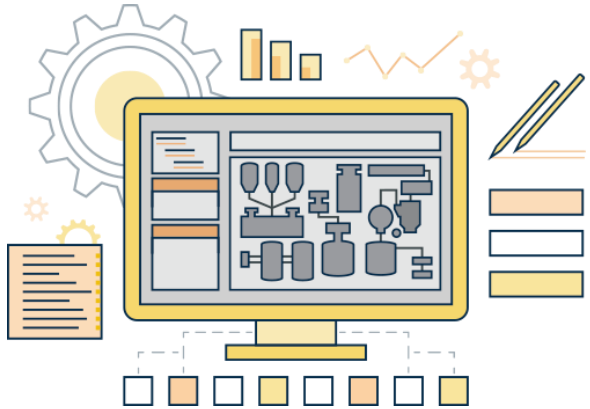
By Ines Gavrilut, Felix Kytzia, Kristina Izmailova, Zeina Najjar, Barbara Koch, Marco Andrés Guevara-Luna, Adrien Barth, Alain Clappier, Nadège Blond, Johannes Miocic, Joris Dehler-Holland, Bushra Canaan

Book Cross-Border Renewable Energy Transitions

Edition	1st Edition
First Published	2021
Imprint	Routledge
Pages	31
eBook ISBN	9781003199977

Share

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Publications:

Accepted conference paper: Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids

The 26th SPEEDAM SORRENTO – ITALY (22-24 June 2022)

speedam

Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids

Bushra CANAAN
IRIMAS URUHA7499
University of Haute Alsace
Mulhouse,France
bushra.canaan@uha.fr
Felis Institute
Albert-LudwingsUniversity
Freiburg, Germany
bushra.canaan@felis.uni-freiburg.de

Bruno.COLICCHIO
IRIMAS URUHA7499
University of Haute Alsace)
Mulhouse, France
bruno.colicchio@uha.fr

Djaffar.OULD ABDESLAM
IRIMAS URUHA7499
University of Haute Alsace)
Mulhouse, France
djaffar.ould-abdeslam@uha.fr

***Abstract*— In this paper, a real-time cyber intrusion detection mechanism based on recurrent neural networks is implemented for detecting cyber-physical attacks targeting AC microgrids (MG). An AutoRegressive eXogenous Neural Network (NARX) model is deployed as an Intelligent Detection System (IDS), to detect cyber-physical anomalies in the behavior of exchanged active power in a connected AC microgrid. Results are validated through a Hardware-in The loop simulation using the Opal RT real-time simulator and an external microcontroller board (Arduino) for Embedding the used Artificial Neural Network ANN.**

Keywords—Cyber-physical security (CPS), Cyber-attacks, Recurrent Neural Network (RNN), Real-time simulation, Hardware-in-the-loop (HIL)

I. INTRODUCTION

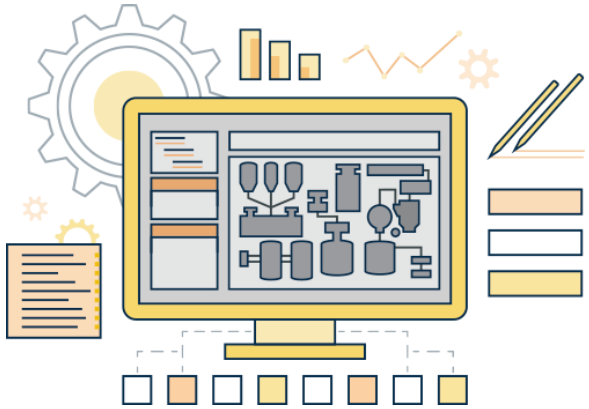
Even though the attack is generated and injected through the application or communication layer, for the physical part of the system, a cyber-attack is still simply an undetected anomaly that drives the systems to exceed its limits.

Anomaly detection, classification and localization in CPSs has been widely explored in literature [5].

Data driven artificial intelligence detection method are getting more and more popular especially in cases of highly complexed systems.

Statistical features extracted from time-series for voltage and current are used in [6] for developing an intelligent anomaly identification technique based on multi-class support vector machines (MSVM). The method was tested and validated under cyber anomalies induced by attacks such as False Data Injection (FDI), Denial of Service (DoS) in

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Events, conferences, and workshops

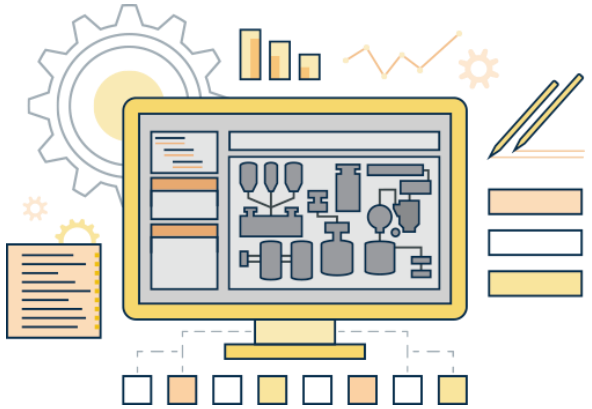
ZHAW: Zurich University of Applied Sciences DynPOWER workshop Winterthur(16 September 2019)

Zurich University of Applied Sciences

zh aw School of Engineering

IMS Institute of Mechatronic Systems

7.2 Predictive models of data security vulnerabilities in the TMO

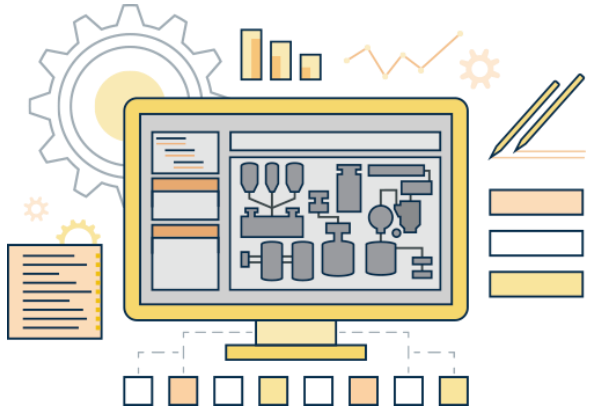


Events, conferences, and workshops

ZHAW: Zurich University of Applied Sciences DynPOWER workshop Winterthur(16 September 2019)

RT Spotlight | Zürich - OPAL-RT: OPAL-RT's Local Conference on Power Systems & Power Electronics Real-Time Simulation (17-18 September 2019)

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Events, conferences, and workshops

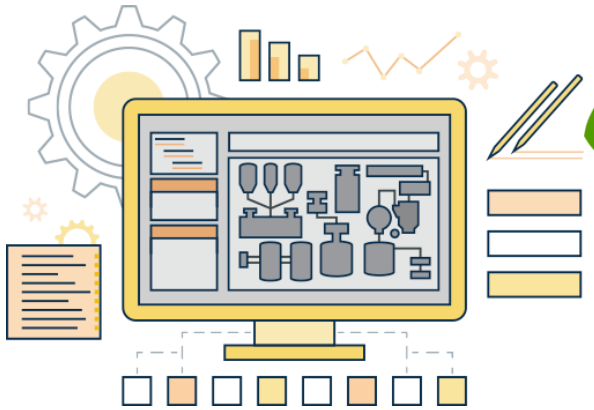
ZHAW: Zurich University of Applied Sciences DynPOWER workshop Winterthur(16 September 2019)

RT Spotlight | Zürich - OPAL-RT: OPAL-RT's Local Conference on Power Systems & Power Electronics Real-Time Simulation (17-18 September 2019)

Sustainable places Rome (28 September-1 October2021)

SUSTAINABLE PLACES 2021
Sep. 29 - Oct. 1, 2021 | Rome, Italy

7.2 Predictive models of data security vulnerabilities in the TMO



RES-TMO

Events, conferences, and workshops

Recommendations

Energy sector actions for Europe’s short-term recovery should be boosted using large-scale programmes for renovation that lifts barriers standing against the full investment in energy projects promoting the clean energy industries and infrastructure of the future.

All relevant EU actors must be ready to respond collectively and disclose pertinent information based on a 'need to share' rather than a 'need to know' premise.

Governments, utilities, and other stakeholders in the power value chain must be proactive in their search for solutions that can adapt to changing cyberthreats. It will be vital to maintain a long-term commitment to cooperation and partnership.

working and elaborating on the standardization enclosure, especially for the most affiliated pieces of the smart grid, becomes an urgent need.

Coordination between Member States is vital in order for Member States to be compliant with the NIS Directive

Cross boarder collaborations

- Two parallel frameworks.

setting up acceptable and efficient governance, with regional cooperation on cyber security topics as a key component.

enables the controlling and securitizing disclosure of vulnerabilities and incidents.

- effective cyber response architecture that will allow for a quick and coordinated reaction in the event of a cyber security emergency.
- improving the energy sector's organisational readiness and protection by addressing the need to improve cyber resilience necessitate a consensus agreement

- Creating a European cyber security maturity framework tailored to the energy industry
- Develop internal coordination and explore international collaboration through mutual experience sharing across borders.

Thank you for listening!