PowerTech Belgrade 2023

LEADING INNOVATIONS FOR RESILIENT & CARBON-NEUTRAL POWER SYSTEMS

25-29 JUNE, 2023, BELGRADE, SERBIA

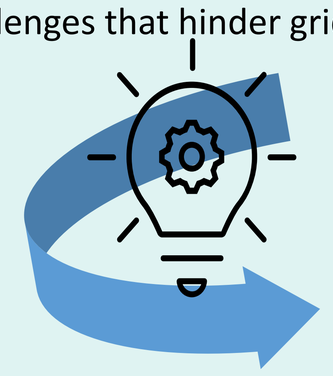
Specifications of a Simulation Framework for Virtualized Intelligent Electronic Devices in Smart Grids covering Networking and Security Requirements

Nadine Kabbara~*, Agrippina Mwangi*, Madeleine Gibescu*, Ali Abedi'', Alexandru Stefanov'', Peter Palensky''

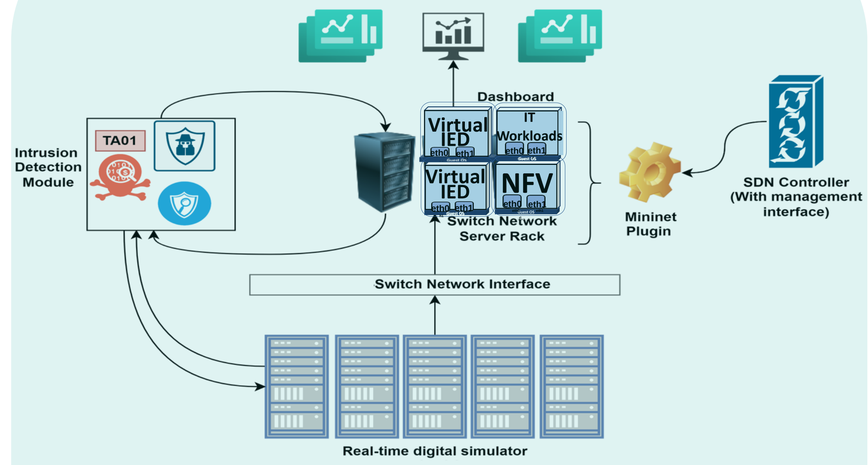
*~EDF R&D, Paris Saclay, France ; *Utrecht University, Netherlands; ''Delft University of Technology, Delft Netherlands*

INTRODUCTION

- Protection, Automation, and Control (PAC) applications are integral elements of cyber-physical power grids → **IT/OT convergence**
- Added technical and economic challenges that hinder grid modernization efforts
  - *Number of devices*
  - *Maintainability & Management*
  - *Difficulty to evolve (flexibility)*



Need for a multidisciplinary simulation framework supporting grid modernization

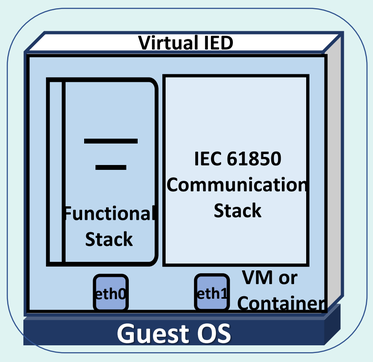


Framework for Virtualized Intelligent Electronic Devices vIEDs including a real-time physical simulator, an SDN controller, and an intrusion detection module.

FRAMEWORK FOR VIRTUALIZED INTELLIGENT ELECTRONIC DEVICES IN SMART GRIDS

The proposed simulation framework serves as an advanced testing and analysis tool for critical cyber-physical power system developments. It comprises of i) vIED setup, ii) software defined networking & network function virtualization (SDN/NFV), and iii) cyber security intrusion detection system (IDS)

i) Virtual IEDs



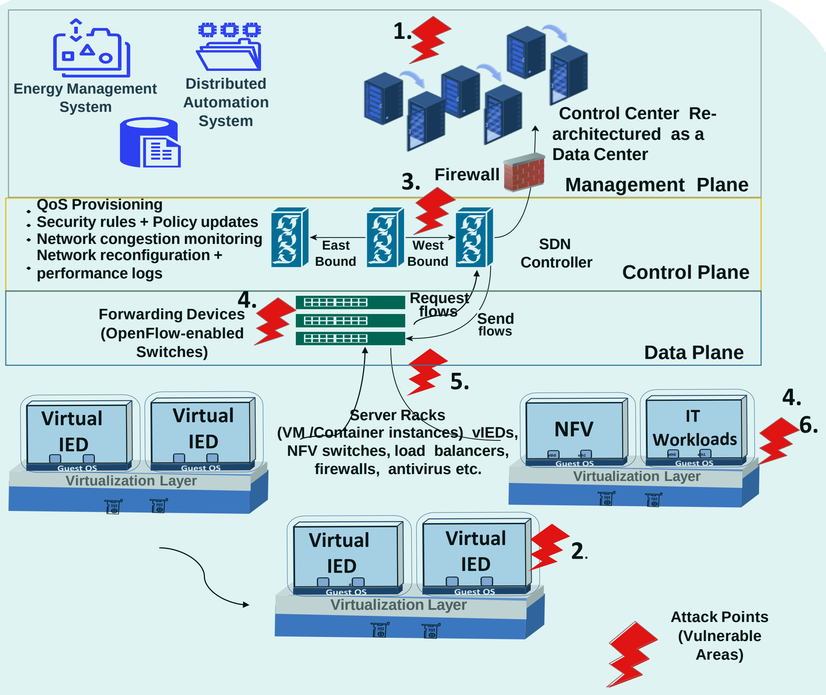
Transitioning to vIEDs is motivated by:

- **Reducing deployment efforts of physical IEDs.**
- **Testing environment equivalent to final deployment setup.**
- **Backup to physical IEDs for inherent redundancy reduce system downtimes.**

ii) SDN/NFV Network Model & QoS

Several performance concerns can be monitored at the level of the SDN controller:

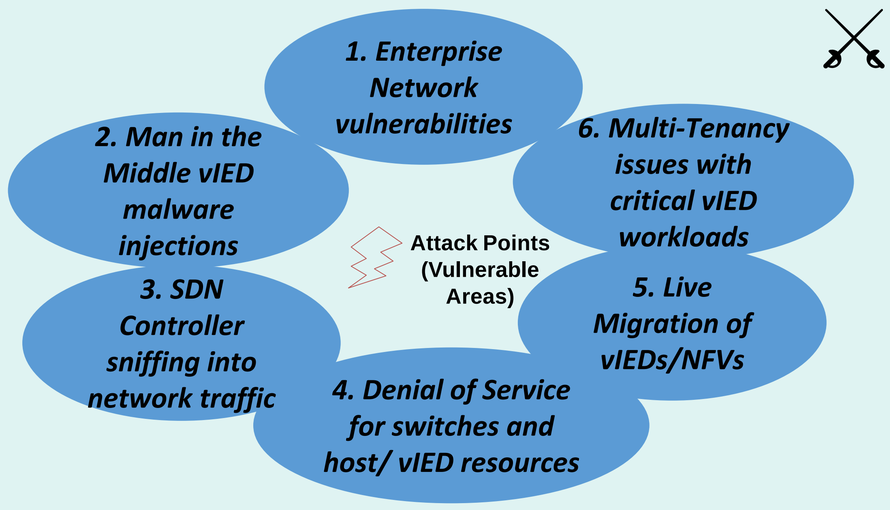
- **Resource Scheduling & Device Failures**
- **Network Congestion & Service loss**



Communication network model managed under the SDN framework and possible attack surfaces.

iii) CYBERSECURITY OF VIED/SDN FRAMEWORK

We analyze the attack surfaces introduced by the proposed framework, starting from the management plane to the vIED racks.

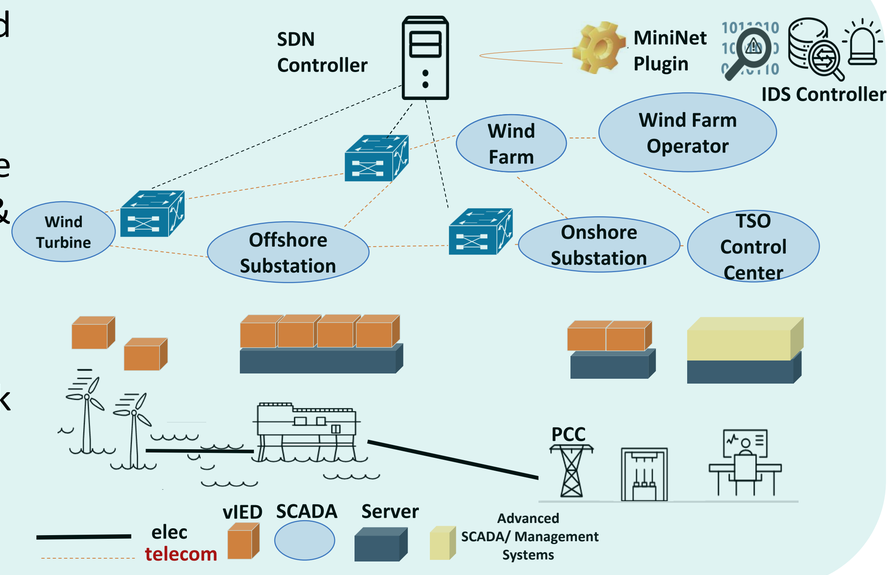


Some countermeasures to the identified attach surfaces:

- **IEC 61850 /62443 implementations**
- **Host-Based Intrusion Detection Systems**
- **Network-Based Intrusion Detection Systems (SDN Controller level)**

OFFSHORE WIND CASE STUDY

- Proprietary physical IEDs are replaced with vIEDs.
- The robust framework ensures the performance of data-in-transit & protection from malicious access.
- Both LAN & WAN cyber attack scenarios are envisioned.



CONCLUSION

- Grid modernization requires extensive testing of the solution's maturity and reliability, especially for networking bottlenecks and security attacks.
- We expect future offshore SCADA systems to co-exist with the advanced SDN and IDS systems.
- Migration of vIEDs due to device maintenance or external anomalies is interesting from an operational perspective yet still poses significant security threats.