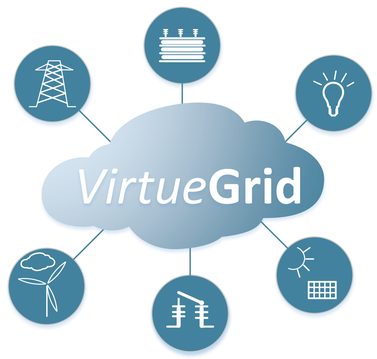
OLIVER JUNG[1] // oliver.jung@ait.ac.at // **MISLAV FINDRIK**[1] // mislav.findrik@ait.ac.at
FRIEDERICH KUPZOG[2] // frriederich.kupzog@ait.ac.at
1. AIT Austrian Institute of Technology GmbH, Center for Digital Safety & Security, Vienna.
2. AIT Austrian Institute of Technology GmbH, Center for Energy, Vienna.

powered by klima+ energie fonds

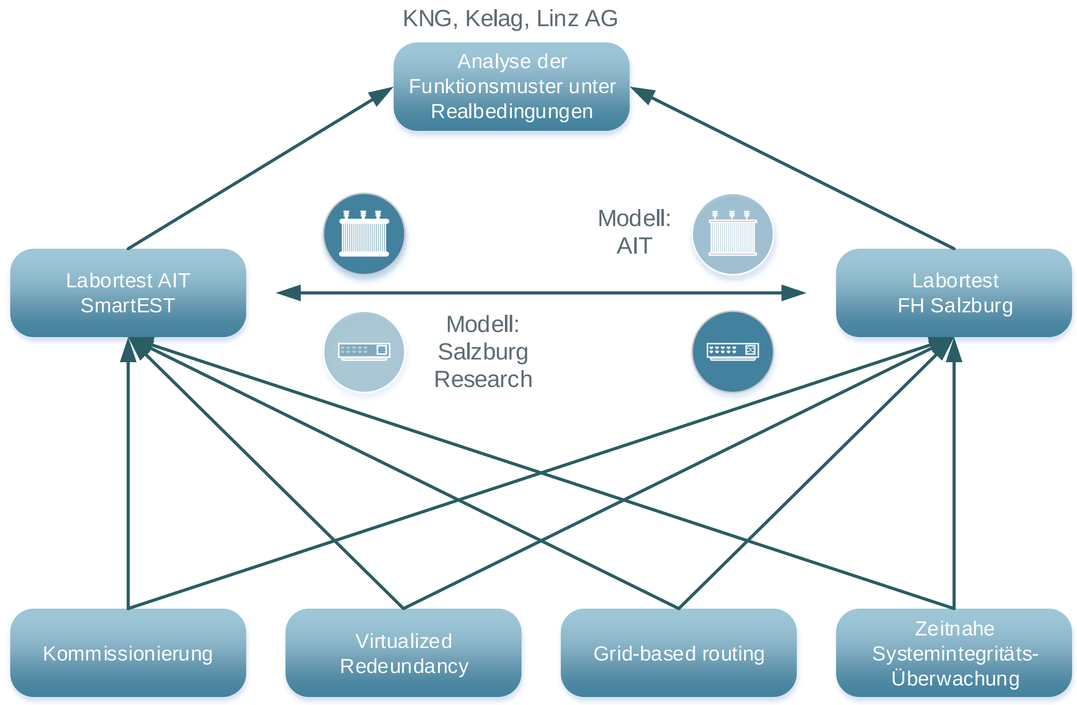
VIRTUEGRID - VIRTUALISIERUNG FÜR RESILIENTE UND SICHERE SMART GRID-KOMMUNIKATIONSNETZE

AIMS OF VIRTUEGRID

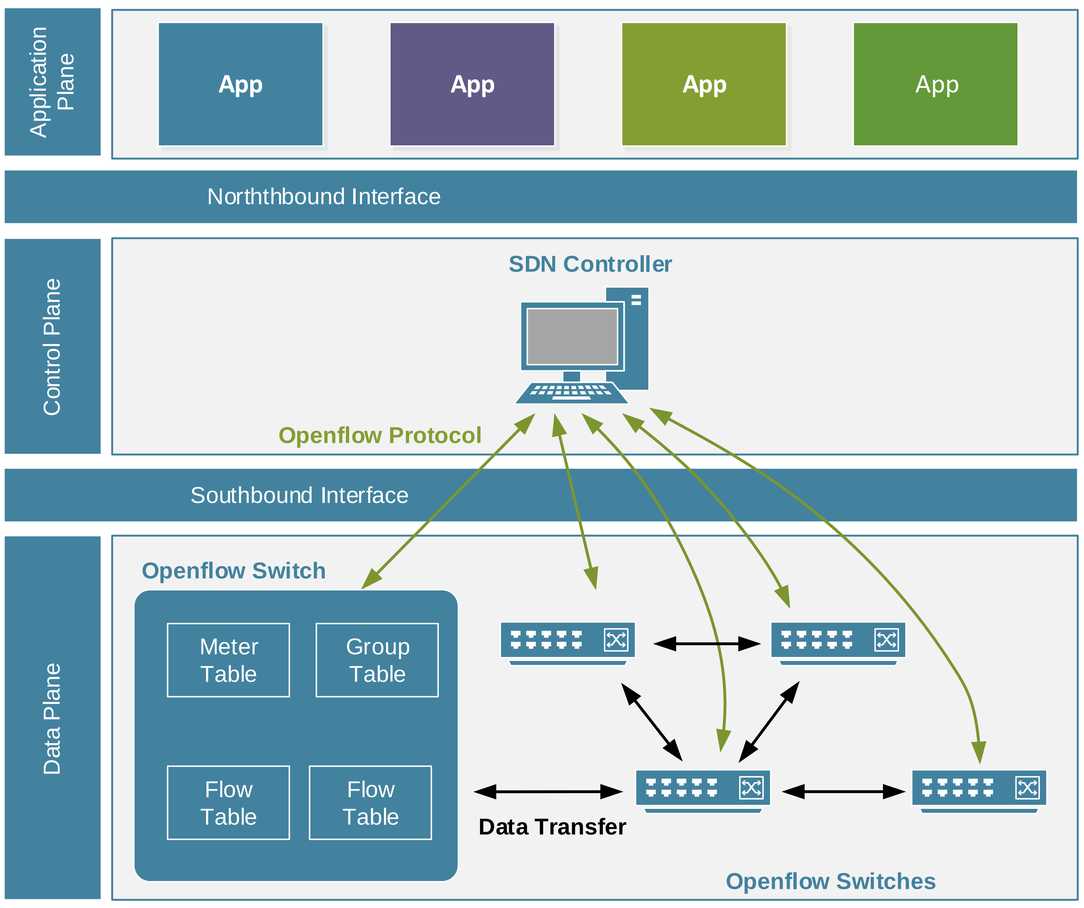


- Evaluate virtualisation concepts as potential solutions to practical core issues in energy grids
- Virtualization technologies for supporting essential future use cases
  - Reducing effort for system (re-)configuration
  - Re-locate decentralized processes in case of maintenance or unplanned interruptions
  - Improve monitoring and situational awareness capabilities in ICT networks for energy grids
- Identify benefits and shortcomings of solutions based on virtualisation concepts

USE CASES



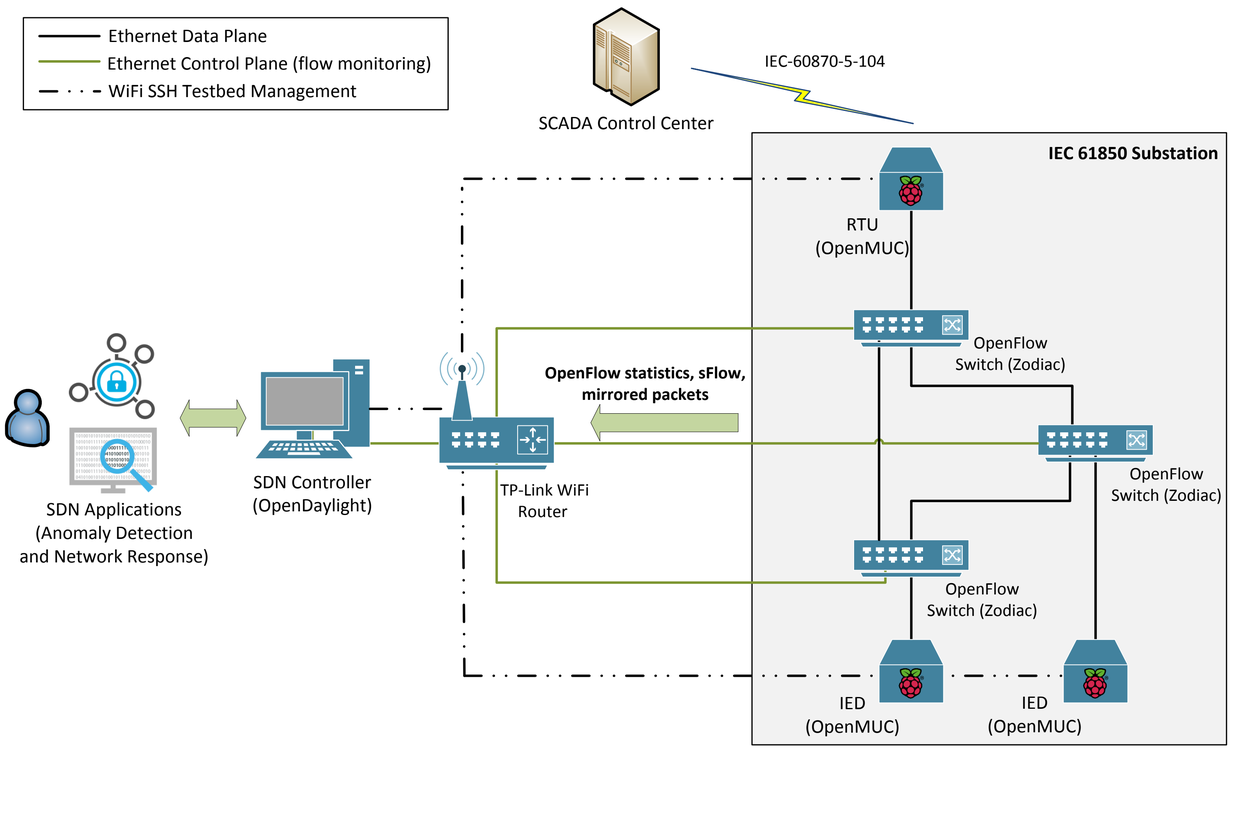
SDN ARCHITECTURE



EXPECTED RESULTS

Use Case	Expected results	Lab Tests	Field Trial
Virtualised Redundancy	Improved redundancy by exploiting SDN functionality	Two redundant autzomation devices, Integrated into a SDN environment	Not yet planned
Commissioning	Scalability and decreased effort	MPLS test bed at Linz AG, additional integration of SDN by VirtueGrid	Linz AG
Grid-based Routing	Simple LV grid simulation (connected graph) that can be re-arranged	Real HW Controller-in-the-loop with regular SDN controller	Stage 1: Deploy substation computers, simulate SDN centrally Stage 2: Emulate SDN by deploying SDN switch to field devices Stage 3: supervised closed loop (vision/wish)
Anomaly Detection	Reliable anomaly detection using (malicious and non-malicious) SDN flow data	Lab test with emulated/simulated data flows	Not yet planned

ANOMALY DETECTION USE CASE



SYSTEM STATUS INFORMATION

- Testbed is designed for **development and verification of SDN cyber-security applications for substations**:
  - Based on OpenFlow-enabled switches, Rasberry Pi‘s with OpenMUC framework, and OpenDaylight controller
  - Designed to mimic functionalities of a secondary substation based on IEC 61850 and IEC 104 protocols
  - Collecting flow information from OpenFlow meters or via sFlow protocol, on demand raw packet anaylsis
- **Design goals** for SDN cyber-security applications:
  - **Anomaly detection**: (i) identify compromised devices or malicious actions based on flow information and behavioural profiles, (ii) detect software/firmware malfunctions or failures
  - **Active response**: (i) isolate compromised devices and deny malicious actions, (ii) link failure recovery

Dieses Projekt wird aus Mitteln des Klima- und Energiefonds gefördert und im Rahmen des Energieforschungsprogramms 2016 durchgeführt.

fhs Fachhochschule Salzburg University of Applied Sciences · Kärnten Netz · kelag · NOKIA SIEMENS · STROM NETZ GMBH LINZ · salzburg research · AIT AUSTRIAN INSTITUTE OF TECHNOLOGY