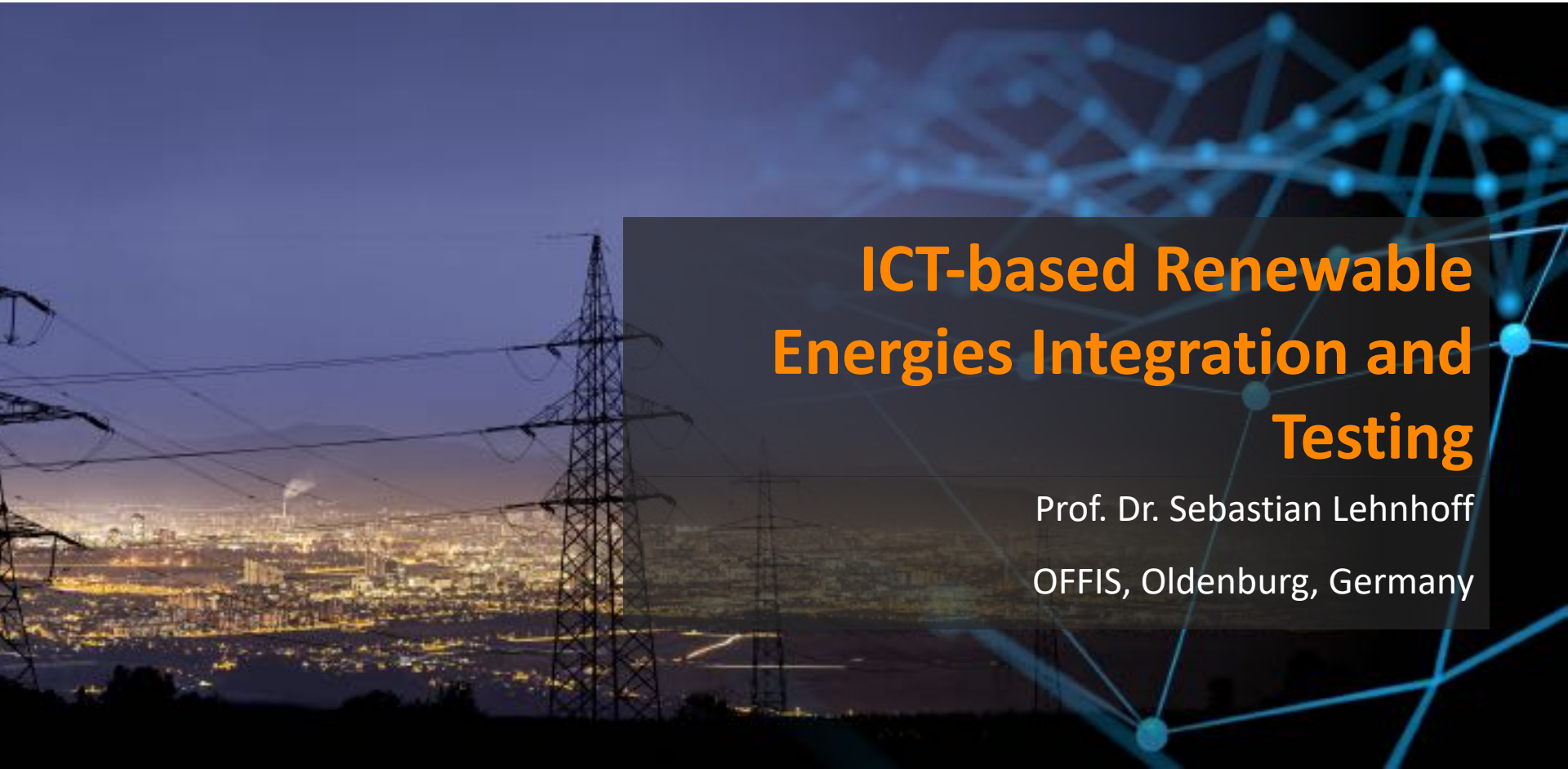


# ICT-based Renewable Energies Integration and Testing

Prof. Dr. Sebastian Lehnhoff

OFFIS, Oldenburg, Germany

# Energy Systems are Cyber-Physical Systems (CPS)

With special characteritics

1. **Regarded as critical infrastructure (KRITIS)**
   > indispensable lifeline of modern societies
2. **Cross-continental size (EU-perspective)**
   > from North Africa to Scandinavia, from Ireland to Asia
3. **Propagation of phenomena and their dynamics**
   > instantaneous propagation velocity of instabilities
4. **Omnipresent conflicts of objectives**
   > monetary, technical, (national/international) political interests
5. **Undergoing rapid and fundamental change...**

# Three Major Trends

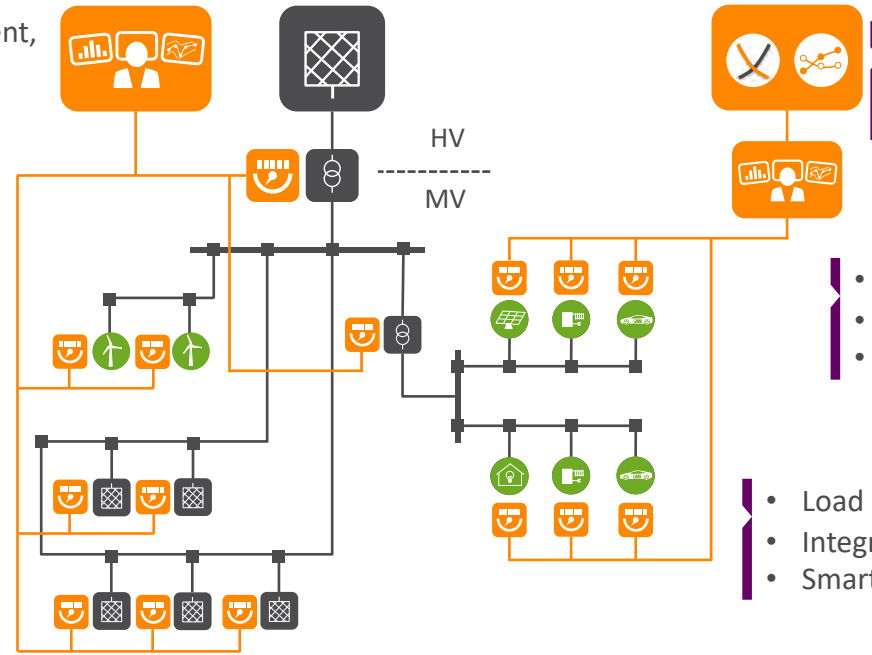
…that influence the stability of KRITIS Energy

1. **Conversion of the energy system, e.g.**
   - > many smaller systems, prone to forecast-errors, system-critical as a whole
   - > networking through digitalization
   - > competition and new business models
2. **Digitization trends, including**
   - > internet of Things (IoT): several billion devices on the Internet and connected to our power grid (televisions, baby monitors, alexa, etc.)
   - > Smart Services, Cloud, Blockchain, Artificial Intelligence, Big Data,...
3. **Susceptibility to new effects, e.g.**
   - > occurrence of "classic" IT challenges (errors, update management, interactions)
   - > sophisticated cyber-attacks (with state-funded resources)

# Energy Systems are Complex Cyber-Physical Systems

Diverse tasks in heterogeneous, distributed (sub)systems under different responsibilities

- Forecast of network conditions,
- Optimized reactive power management,
- Detection of anomalies in power and communication networks.




- Algorithmic energy trading,
- Market integration of renewable energies.

- Virtual power plants,
- multi-modal optimization,
- Sector coupling.

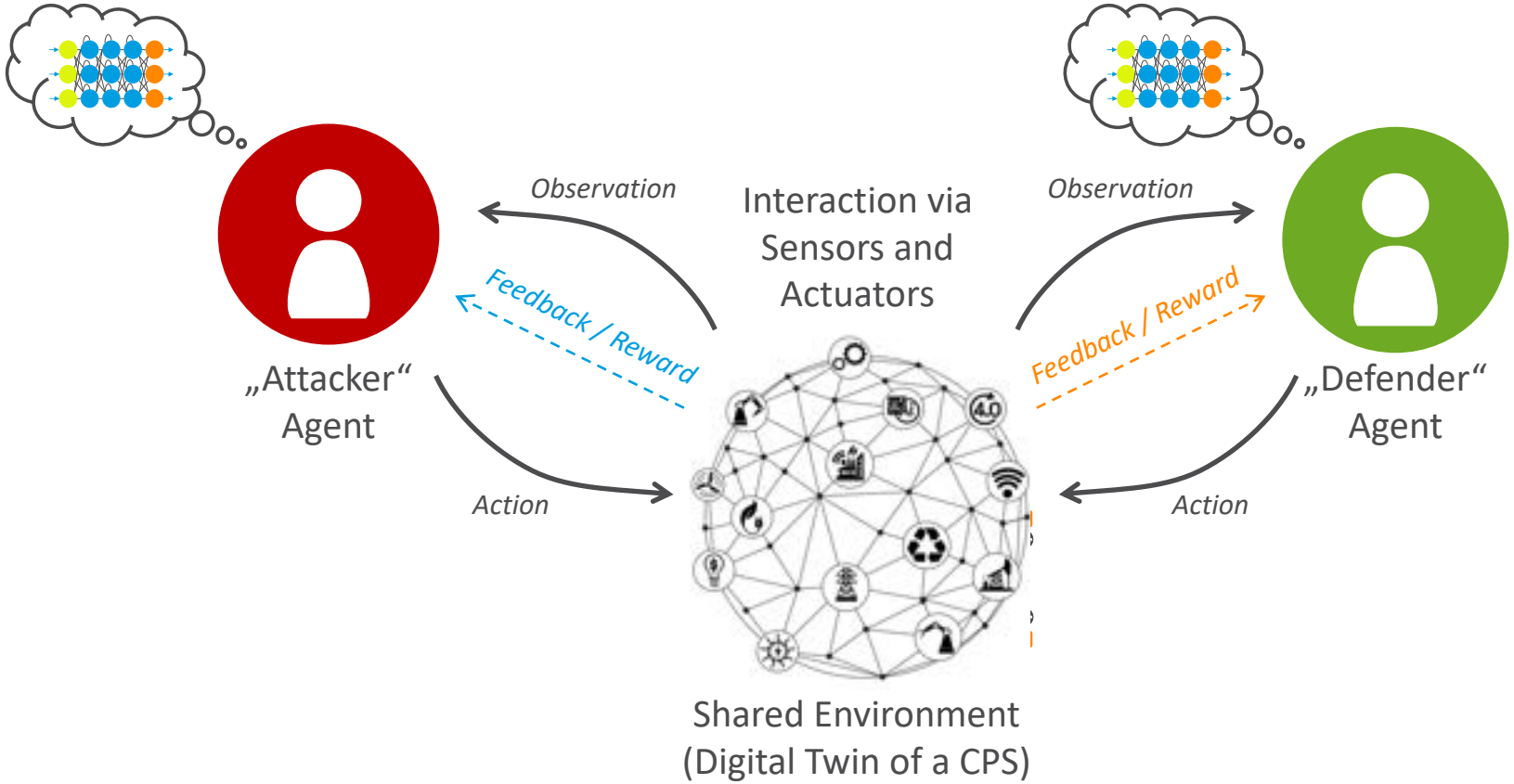
- Monitoring of the operating states,
- Automation yellow traffic light phase,
- decentralised system services.

- Load and flexibility management,
- Integration of end customers,
- Smart metering.

***A wide range of error-sources/entry-points into a safety-critical infrastructure...***

# AI-based Testing (Adversarial Resilience Learning)

Competing agents explore vulnerabilities by interacting on a shared environment



# Use Case: Resilient Systems Testing/Analysis and Training

Variations of Adversarial Resilience Learning

**Testing/Analysis – only Attacker**

- Test laboratory for resilient systems
  - (ICT-)device testing
  - attacker explores vulnerabilities
  - ”conquest" of the system

**Training – Attacker and Defender**

- AI for automated operation
- Resilience strategies of the overall system
  - Attacker trains defender

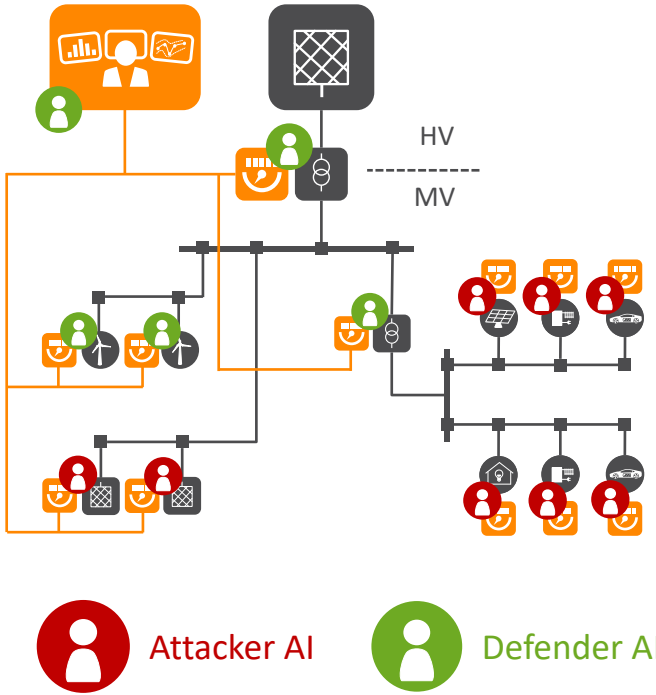
**“Attacks“ not only malicious**, but also complex dynamics & environmental factors

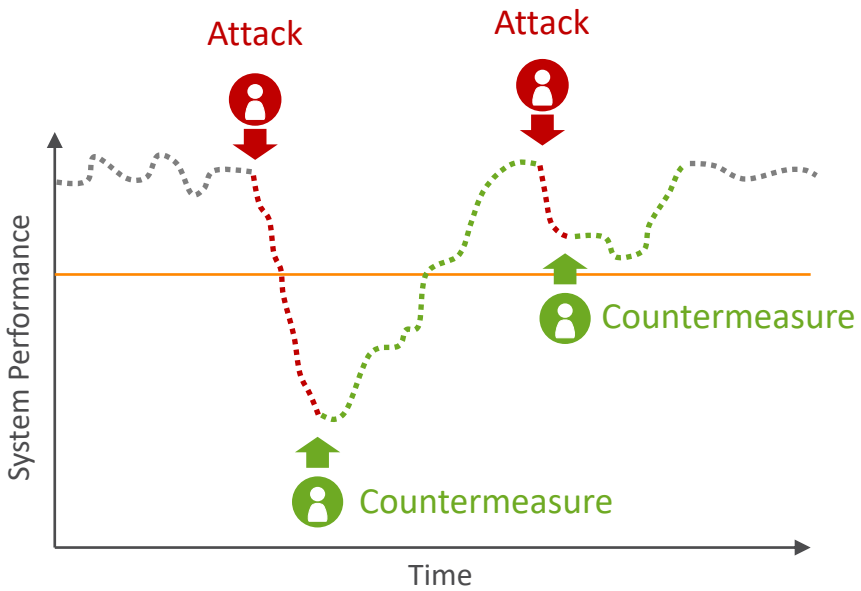
- forecast deviations
- damage caused by accidents etc.
- dynamic interactions (*from inefficient over ineffective to instable*)

# Demo: Cyber-Attack on a Power System

## Prevention of (sub-)system takeover as a secondary problem

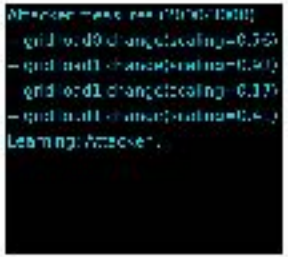
Smart Grid
Cyber-Resilience Lab



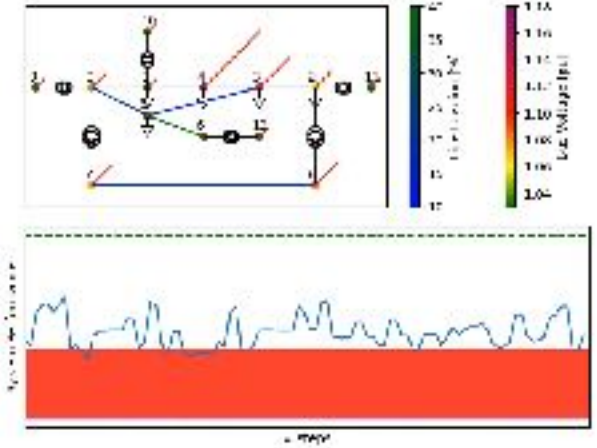
# Demonstrator für Adversarial Resilience Learning

## KI-basierte Analyse der Resilienz von Smart Grids



Attacker Score:

0



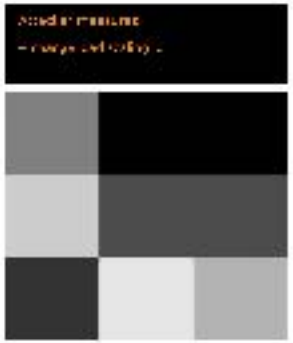


Defender Score:

0

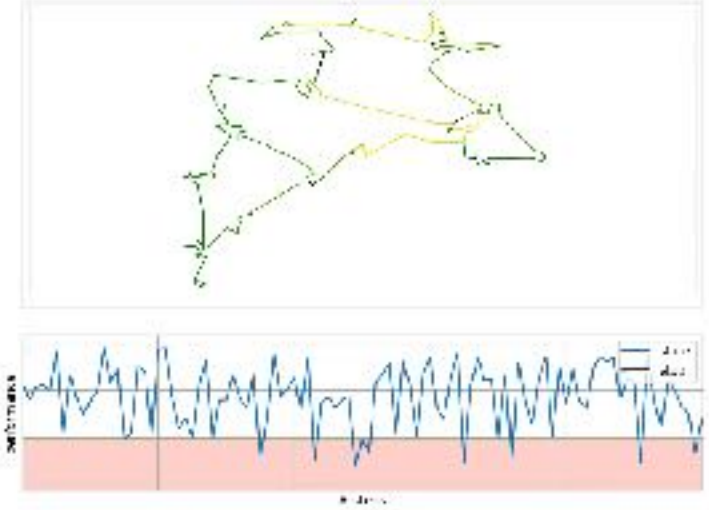
# Demonstrator für Adversarial Resilience Learning

## KI-basierte Analyse der Resilienz von Smart Grids



Attacker score

0



Defender score

1

# Conclusion and Outlook

Artificial Intelligence (AI) in testing and Adversarial Resilience Learning (ARL)

**Traditional means/methods have been proven to miss:**

> vulnerabilities to interdependent/dynamic failures

> specialized/targeted attacks

**ARL as an AI-based game-theoretic approach to vulnerability testing (CPS modelling)**

> resilient operation of interconnected systems

> equilibria more relevant than “absolute” safety

**There is no way back from digitalized energy systems!**

> most promising answer against on-line dynamics and highly specialized/targeted attacks is *Operational Flexibility (on-line change of system characteristics)*

**Smart Grid Cyber-Resilience Lab**