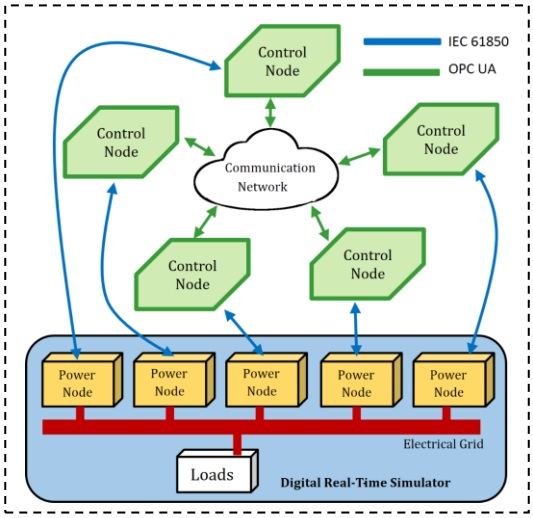
TRANSNATIONAL ACCESS
USER PROJECT FACT SHEET

USER PROJECT	
Acronym	OpenDISCO
Title	**OPEN**-Source Security Assessment Framework for **DIS**tributed **CO**ntrol in the Smart Energy Grid
ERIGrid Reference	
TA Call No.	**4**

HOST RESEARCH INFRASTRUCTURE			
Name	University of Strathclyde D-NAP Dynamic Power Systems Lab		
Country	**Scotland, U.K.**		
Start date	**3rd of September 2018**	**Nº of Access days**	**8**
End date	**5th of October 2018**	**Nº of Stay days**	**12**

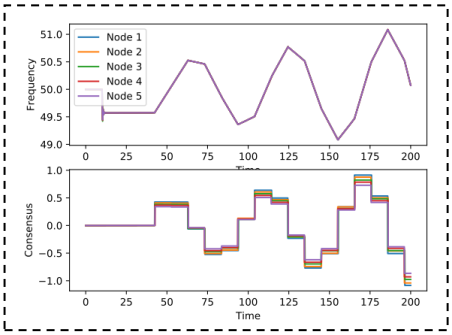
USER GROUP	
Name (Leader)	Marius Stübs
Organization (Leader)	Universität Hamburg
Country (Leader)	Germany
Name	Kevin Köster
Organization	Universität Hamburg
Country	Germany
Name	
Organization	
Country	
Name	
Organization	
Country	

1. USER PROJECT SUMMARY (objectives, set-up, methodology, approach, motivation)



The project group from the University of Hamburg is currently developing a distributed security assessment framework with the focus on Smart Grid applications.
The main objective of the transnational laboratory access was to show the capabilities of the framework in a realistic scenario. The experiment was set up as a controller-hardware-in-the-loop environment, thereby investigating the effects of denial-of-service attacks on a reference implementation of distributed scheduling scheme, controlling the frequency of an islanded microgrid simulated on a real-time digital simulator, as configured with Matlab.
Regarding the methodology, the distributed framework nodes were configured to apply denial-of-service attacks of increasing severity (1ms to 10 seconds). The effect of the cyber-physical system was recorded. One distinguishing feature of the framework is its decentralization: Thus, the investigated effects where introduced independently on every node in the network, enabling high scalability of the approach.

2. MAIN ACHIEVEMENTS (results, conclusions, lessons learned)



The decision, to run the controller software on Raspberry PI embedded devices added to the confirmation, that the developed framework is indeed capable of real-time control, as well as decentralized DOS simulation and to support attack detection.
The investigated control scheme was found to be robust against typical communications delays, but when systematically applying the possible effects of targeted DOS-attacks, the stability of the microgrid frequency was strongly imbalanced.

3. PLANNED DISSEMINATION OF RESULTS (journals, conferences, others)

The results of the TA have led to joint submission of both working groups in Hamburg and Glasgow to be accepted at CIRED 2019.

The research group is continuing the started work, using screen sharing and voice-over-IP technologies, to even conduct further research towards evaluating the robustness of investicated distributed control algorithm when executed using Power-Line-Communication and is planning a to submit a publication in Spring 2019 in ISGT Europe 2019.