Notes on Completion: Please refer to the appropriate NIA Governance Document to assist in the completion of this form. The full completed submission should not exceed 6 pages in total.
Network Licensees must publish the required Project Progress information on the Smarter Networks Portal by 31st July 2014 and each year thereafter. The Network Licensee(s) must publish Project Progress information for each NIA Project that has developed new learning in the preceding relevant year.

NIA Project Close Down Report Document

Date of Submission

Feb 2025

Project Reference Number

NIA2_NGESO018

Project Progress

Project Title

Automated Identification of Sub-Synchronous Oscillations (SSO) Events

Project Reference Number

NIA2_NGESO018

Funding Licensee(s)

NESO - National Energy System Operator

Project Start Date

September 2022

Project Duration

1 year and 7 months

Nominated Project Contact(s)

Sami Abdelrahman (NGESO)

Scope

New transmission network connections are checked for Sub-synchronous Oscillations (SSO) based on a few future network conditions. Due to the inherent uncertainties in the network and forthcoming reinforcements, scenarios other than those currently considered could materialise. These uncertainties, and the possibility of more frequent controller interactions, are due to the changing nature of the future system with a more significant proportion of converter interfaced generation (of different technology types) coupled with declining short circuit level.

As the SSO identification requires Electromagnetic Transient (EMT) analysis, which is very time-consuming, there is a need to develop an analytical framework that will allow screening of scenarios without running EMT simulations and reduce the total number of scenarios that need to be investigated further. This will ensure that EMT simulations are used only for scenarios of potential concern, and system engineers can focus on root cause analysis. Due to the volume of studies, the process' complexity and the amount of data generated, it is crucial to automat this process as much as possible.

Objectives

The project aims to apply a few advanced techniques borrowed from mathematics, statistics, and machine learning to solve the complex problem of identifying and managing SSOs in future power systems. The project will aim to deliver the following objectives:

- A primary objective of this project is to represent the black box models by a grey box approach which will allow for the identification of state variables which participate and contribute to the poorly damped oscillations. This is crucial to facilitate root cause analysis of controller interaction events.
- Develop a methodology to filter from an extensive a pool of scenarios with the possibility of SSO events based on impedance scans techniques.

- Develop a tool combining automation and machine learning techniques to run EMT simulations unattended and to identify SSO events automatically.
- Provide study cases to evaluate the performance and accuracy of the tools by testing historical event data or synthetic data created by simulation.

Success Criteria

- A framework to reduce the overall time and effort required to investigate a wide range of scenarios for potential SSO threats arising from new transmission connections.
- The ability to incorporate different sources of uncertainty in the scenario analysis.
- An approach for root cause analysis of SSO events in networks with proprietary controllers.
- An automated SSO identification process using time-domain results from PSCAD.
- Dissemination and training for the learnings and tools developed in the project.

Performance Compared to the Original Project Aims, Objectives and Success Criteria

National Grid Electricity System Operator ("NGESO") has endeavoured to prepare the published report ("Report") in respect of Automated Identification of Sub-Synchronous Oscillations (SSO) Events, NIA2_NGESO018 ("Project") in a manner which is, as far as possible, objective, using information collected and compiled by NG and its Project partners ("Publishers"). Any intellectual property rights developed in the course of the Project and used in the Report shall be owned by the Publishers (as agreed between NG and the Project partners).

The Report provided is for information only and viewers of the Report should not place any reliance on any of the contents of this Report including (without limitation) any data, recommendations or conclusions and should take all appropriate steps to verify this information before acting upon it and rely on their own information. None of the Publishers nor its affiliated companies make any representations nor give any warranties or undertakings in relation to the content of the Report in relation to the quality, accuracy, completeness or fitness for purpose of such content. To the fullest extent permitted by law, the Publishers shall not be liable howsoever arising (including negligence) in respect of or in relation to any reliance on information contained in the Report

The project was delivered in four work packages. All the work packages WP1, WP2, WP3 and WP4 have been delivered and can be accessed through ENA portal (https://smarter.energynetworks.org). The scope of these work packages is summarised below:

WP1 - Review of methods
Assess strengths and weaknesses of existing frequency domain analysis techniques including implementation challenges and compatibility with large practical networks.
Develop novel methodologies for frequency domain analysis of controller interactions specifically focusing on approaches to deal with proprietary black box models. Explore different screening approaches for priority ranking of critical uncertain parameters.
Compare machine learning techniques to find a suitable classification algorithm for the automated identification of SSO events from time domain simulation results.
Review existing (time-domain) modelling tools for operational stability margin, inputs and assumptions for controller interaction studies and the associated business processes (engagement with ESO/NGET subject matter experts)
Review learning from other ESO and industry innovation projects

WP2 - Development and testing of methods
Define appropriate case studies and test networks (and operational scenarios) to test the performance of the developed methods of frequency scanning, uncertainty sensitivities and classification of SSO scenarios.
Develop and trial the most promising methods from WP1 on test networks in PSCAD, explore sensitivity and automation techniques to reduce computational resource. Algorithms will be implemented in Python and linked to PSCAD.
Compare and verify the method results e.g., based on available measurements of events or published results from other research and networks events

WP3 – SSO Tool Demonstration
Adapt the automation code for a ESO submitted network model (South East coast) with no User EMT models.
Test the performance of SSO tool including grey box approach on the South East coast network with proprietary models
Demonstrate SSO tool performance in Cigre Benchmark test system
Validate and compare the performance of SSO tool (Beta version) with another scan tool from MHI

WP4 – SSO Tool Implementation Plan

Discuss implementation Plan for the tool to be used by Wider Teams

Performance Comparison

Future work

In WP1, a literature review report was delivered, including collecting all documented SSO events from around the world that are publicly available. Also, in WP1, a comparison between classification techniques was undertaken and the most promising classifier in terms of performance measures was selected and further developed to classify SSO events from synthetic data.

In WP2, a Cigre Benchmark test system was acquired from the relevant Cigre working group and migrated from MATLAB Simulink into PSCAD. The modelled SSO events were validated and compared to the published Cigre data from the MATLAB benchmark system. A frequency scan tool was developed in PSCAD and tested in the Cigre Benchmark. The Grey Box technique was developed in python and incorporated in the main tool. A PSCAD automation module is developed in Python to interface with the PSCAD API. This automation module enables users to define several operational scenarios through the interactive user interface and apply the changes to the network model in PSCAD.

In WP3, the SSO tool was adapted for proprietary models on Southeast Coast (SEC) network. Grey box method was tested on the network with multiple proprietary models nearby. The Beta version of the SSO tool was submitted to ESO for validation and testing on ESO network models. First, the performance of the SSO tool was validated in a network with known resonant frequency. The SSO tool was then compared with another frequency scan tool from Manitoba Hydro International (developer of PSCAD) to validate performance on other networks and models. Lastly, the SSO tool was tested in the ESO SEC network. The installation details and steps required to use the front end of the SSO tool was described in WP3 report along with validation and comparison results. A WP3 workshop was conducted to showcase the highlights and work done so far.

In WP4, results from the comparison with MHI tool is documented providing evidence of validation. Requirements of the source code to be in line with PEP guidelines have been addressed. The source code architecture and documentation were discussed in terms of its ability to be used during the development as BAU phase. Future modifications or scope has been documented in the WP4 report.

Required Modifications to the Planned Approach During the Course of the Project

No modifications required to the planned approach.

Lessons Learnt for Future Projects

The lessons learnt are:

As per the original scope of the project, a graphical user interface (GUI) was developed in WP3 phase. However, no guidelines were communicated to the partner covering the guideline with which the GUI was to be developed. Consequently, the interface was developed based on JAVA script (with web interface) which turned out to be unacceptable to NESO's IT security team. This necessitates the requirement of IT Security to be involved in earlier stages of projects of this nature in future.

Sharing of User Models or the GB network model turned out to be extremely difficult considering NDA concerns. For future projects, such requirements can be anticipated early to minimize delay.

There was difficulty in sharing the required online measurement data or the possibility of generating synthetic data that can accurately reflect the field measurements. Consequently, it was not possible to validate the performance of the tool for its ability to automatically detect SSO scenario from the PMU measurement data.

The availability of the test systems in the required tools and format was a challenge. At the time of development and testing of the tool, there were no standard test systems available in the target software platform (PSCAD) to validate the performance of the tool. The test system that was available was on another software platform (MATLAB). Considerable effort was made to convert the test system from MATLAB to PSCAD. In future in similar projects, development of the test system in PSCAD should be considered in earlier stages.

The testing of the beta version of the tool in the NESO systems while being developed allowed for the early identification of IT and security requirements issues. This facilitated the final delivery and handover of the tools by the end of the project.

Note: The following sections are only required for those projects which have been completed since 1st April 2013, or since the previous Project Progress information was reported.

The Outcomes of the Project

The project has delivered a python-based tool that can automate screening of potential SSO related scenarios in system planning studies.

Key outputs include a delivery of frequency scan component that can be used with PSCAD for obtaining impedance profile of apparatus and grid and python scripts. The python scripts automate the impedance scanning process, has different assessment criteria to evaluate critical sub-synchronous oscillations (SSO) scenarios. The python script also has grey box algorithm incorporated which provides a detailed insight into the SSO issues, allows system modes identification without developing the system 'A' matrix analytically. This is particularly useful for practical studies as User models for converters are always 'Blackbox' to protect trade secrets. Currently, this algorithm is only modelled and available in this tool. Additionally, the python script has a module for automatic detection of sub-synchronous oscillations in the offline simulation results using machine learning techniques. Instead of manually sifting through hundreds of results, the machine learning model can quickly identify SSO in system variables such as voltage, currents, and power. The python scripts have been scanned and approved by our IT security team to be able to use it within our local machines. The frequency scan component and the python scripts were validated by NESO in different environments including a wider EMT GB model with Vendor black-boxed models. A workshop was organized in March 2024 to a wider audience within NESO for demonstration of results and feedback. The workshop was a successful event in terms of the positive response.

These scripts can be particularly useful to our offline modelling team, especially the EMT team in assessing the impact of new connections in terms of their interaction with the GB network. Currently, enhancements have been identified, and the development of the tool as BAU is being discussed with DD&T team.

Data Access

Details on how network or consumption data arising in the course of NIA funded projects can be requested by interested parties, and the terms on which such data will be made available by National Grid can be found in our publicly available “Data sharing policy related to NIC/NIA projects” and www.nationalgrideso.com/innovation.

National Grid Electricity System Operator already publishes much of the data arising from our NIC/NIA projects at www.smarternetworks.org. You may wish to check this website before making an application under this policy, in case the data which you are seeking has already been published.

Foreground IPR

- Extended literature review report including all documented SSO events worldwide
- A python-based tool automating the PSCAD scenario creation and simulation. The current version of the tool includes:

Frequency scan screening tool
Grey box implementation
Multi scenario runs results visualization

Planned Implementation

Based on the testing and validation of the tool, list of potential improvements to the tool was prepared. These are being considered by NESO through a separate Digital Data and Technology project.

Net Benefit Statement

The project would enable a significantly improved characterisation and management of complex dynamics of the evolving electricity system. Some of the immediate and direct benefits would be improved computation time for Electromagnetic Transient (EMT) type studies and the ability to scan a wider pool of scenarios. A major impediment to an exhaustive search of potential scenarios of concern is the inherent computational burden of EMT simulations. In addition to this, the massive amount of data generated from the scenarios are difficult to process, navigate and analyse without an automated framework. The project provides solutions to overcome these challenges through the use of advanced frequency domain techniques. Some of the other key benefits include its usefulness in both planning and connections studies for NESO, TO and customers and wider system analysis for oscillation management.

Other Comments

The Project outcomes and results contain confidential information and intellectual property rights that cannot be disclosed in this Report due to their proprietary nature. Should the viewer of this Report (“Viewer”) require further details this may be provided on a case-by-case basis following consultation of all Publishers. In the event such further information is provided each and any Publisher that owns such confidential information or intellectual property rights shall be entitled to request the Viewer enter into terms that govern the sharing of such confidential information and/ or intellectual property rights including where appropriate formal licence terms or confidentiality provisions. Dependent upon the nature of such request the Publishers may be entitled to request a fee from the Viewer in respect of such confidential information or intellectual property rights

Standards Documents

N/A