European Research Infrastructure supporting Smart Grid and Smart Energy Systems Research, Technology Development, Validation and Roll Out – Second Edition

Project Acronym: **ERIGrid 2.0**

Project Number: **870620**

Technical Report Lab Access User Project

Cyber attack in PV sysTem for voltagE regulation in diStribution neTwork (CybTEST)

Access Duration: 02/06/2022 to 03/07/2022

Funding Instrument:	Research and Innovation Action
Call:	H2020-INFRAIA-2019-1
Call Topic:	INFRAIA-01-2018-2019 Integrating Activities for Advanced Communities
Project Start:	1 April 2020
Project Duration:	54 months
User Group Leader:	Seema Yadav (MNNIT)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 870620.

Report Information

Document Administrative Information	
Project Acronym:	ERIGrid 2.0
Project Number:	870620
Access Project Number:	132
Access Project Acronym:	CybTEST
Access Project Name:	**Cyb**er attack in PV sys**T**em for voltag**E** regulation in di**S**tribution ne**T**work
User Group Leader:	Seema Yadav (MNNIT)
Document Identifier:	ERIGrid2-Report-Lab-Access-User-Project-AccessProjectAcronym-draft-vn.n
Report Version:	V2.0
Contractual Date:	dd/mm/yyyy
Report Submission Date:	03/09/2022
Lead Author(s):	Seema Yadav (MNNIT)
Co-author(s):	Nand Kishor (Østfold University College), Shubhi Purwar (MNNIT)
Keywords:	Cyber-physical security,Switching sliding mode control, attack algorithm, detection, European Union (EU), H2020, Project, ERIGrid 2.0, GA 870620
Status:	final

Change Log

Date	Version	Author/Editor	Summary of Changes Made
28/08/2022	v1.0	Nand	Draft report template
30/08/2022	V2.0	Seema	Addition of appendix

Table of Contents

List of Figures

List of Tables

List of Abbreviations

CO	Project Coordinator
EC	European Commission
LA	Lab Access
UG	User Group
UP	User Project
VSS	Variable Structure System
TCP/IP	Transmission Control Protocol/ Internet Protocol
IEEE	Institute of Electrical and Electronics Engineering
SCADA	Supervisory Control and Data Acquisition
IEC	International Electro technical Commission
O1,O2,O3	Objective 1, 2,3
RTDS	Real Time Digital Simulator
MATLAB	Matrix Laboratory
PMU	Phasor Measurement Unit
CB	Circuit Breaker
DAT	Data file
S(x)	Sliding Surface
CBR_57	Circuit Breaker 57
CBR_79	Circuit Breaker 79
L5,L6,L8	Load 5, Load 6, Load 8

Executive Summary

The sizeable practical power system networks are prone to cyber-physical attacks. The cyber-physical system is integration of physical and communication layer for advance control and self –monitoring techniques, optimisation of assets use, advanced fault detection and mitigation, facilitation of distributed generation and electric vehicle. The archetypical diagram of cyber-physical system is shown in Figure 1. However, exposure of physical system to communication system is main source of cyber-physical attacks. The studies to various kinds of cyber-physical attacks are limited to the type of system and type of cyber-physical attack construction. The detection and mitigation techniques are only designed for conventional energy resources and malware intrusion into the system.

The detection and mitigation of cyber-physical attack can be achieved on the condition that the nature of the attack is exhaustively studied. The switching sliding mode attack construction provides a way to stealthy attack. The foundation of sliding mode attack is variable structure theory that consists of set of continuous subsystems with proper switching logic/algorithm and, as a result, control actions remain discontinuous functions of system state disturbances and reference inputs. The core idea of designing VSS control algorithm consists of enforcing this type of motion in some form of manifolds in system state spaces.

Therefore, in the present study, switching sliding mode attack construction involves enforcing the state variables of power network towards instability in a particular form of manifolds (sliding surface) by changing the status of circuit breaker [1].

The study and analysis of switching sliding attack construction was made possible by imitating the behaviour of intruder. The intruder could remotely connected and intrude in the system over TCP/IP communication protocols. These protocols establish a connection similar to pipeline theory. The intruder design sliding surface and switching algorithm was introduced in the system by means of TCP/IP socket.

The switching stage involves two attributes in the algorithm i.e. “start” and “stop” time of switching based on intruder designed sliding surface. The start- and stop-time of switching sliding mode attack is graphically analysed via phase-portrait plot as shown in Figure 2. The said plot is a graphical representation of rotor angle and rotor speed of the generator. The start-time and stop-time is selected such that the intruder applies the attack in a swiftly and stealthy manner.

The algorithm based on switching sliding surface for attack construction is tested on IEEE 9-bus system. The successful implementation of attack algorithm shows its commendable yet disastrous nature on leading to generator instability.

The study forms a basis for understanding the generator behaviour, at the time of cyber-attack and thus the approach can helpful to devise its detection and mitigation techniques.

The study related to impact of cyber-attack in the control loop of PV systems integrated in distributed network could not be carried out during the visit. This is due to the fact, that we wished to first implement the attack construction algorithm on transmission network, i.e. standard test network, for which model was already available in the RSCAD software.

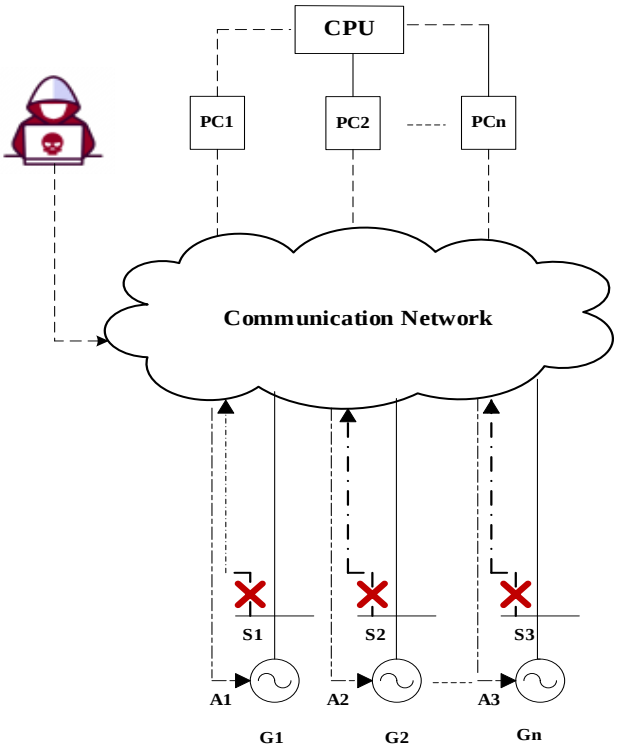


Figure 1 Archetypical diagram of cyber-physical system

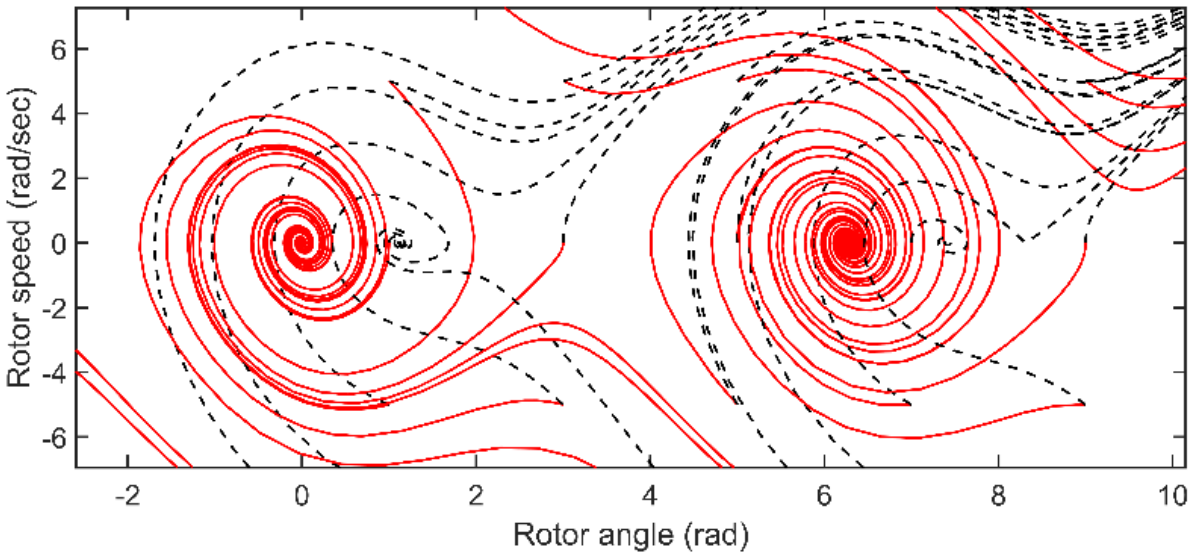


Figure 2 Overlapping phase-portrait of test system

1 Lab-Access User Project Information

1.1 Overview

The VTT IntelligentEnergy testbed is equipped with a local SCADA enabling monitoring and control, RTDS with current and voltage amplifier, communication emulator, and IEC 61850-based control and protection system.

The CybTEST (Cyber-attack in PV system for voltage regulation in distribution system) is primarily construction and implementation of cyber-physical attack in Real-Time Digital Simulator provided by VTT Lab under ERIGrid 2.0 project in the time duration of one month with the help of Seema Yadav, Shubhi Purwar, Nand Kishor and Petra Raussi (VTT) et al. The project CybTEST was conducted with visit of Seema Yadav from 2.06.2022 to 3.07.2022. During the final phase, i.e. 27.06.2022 to 01.07.2022, other two group members; Shubhi Purwar and Nand Kishor visited the VTT lab.

The project was divided into three main phases. In the first phase, the IEEE 9-bus system was configured (operating single and three-phase circuit breakers), and MATLAB code was designed for attack construction. In the second phase, the interfacing of RTDS and MATLAB was examined using various communication protocols, including IEC 61850, GTNET port DNP server, and TCP/IP socket communication with the help of VTT member Mikael Opas. The TCP/IP socket communication is selected for further used studies. The real-time simulation under various cases was planned, executed, observed and compiled with the help of group members.

1.2 Research Motivation, Objectives, and Scope

Motivation:
The Author's research motivation is to apprise system engineers about the most basic yet discreet kind of cyber-physical attack. Switching sliding attack is nothing but a change of status of the circuit-breaker at a definite time instant and for a definite time duration (definite start-and stop-time). Therefore, the project's objective was to develop technical foundations towards attack construction using sliding mode control theory and to understand the severity caused on generator stability at the time of attack.
Objectives: The objectives of the project were:

O1: To formulate sliding mode control theory for cyber-attack construction.

O2: To interface the RTDS/RSCAD with MATLAB platform and implement successful run of the algorithm

O3: To analyse the test-bed at the time of cyber-attack, with changes in operating conditions of power system.

The above-specified objectives; O1, O2 and O3 will help in better understanding the consequences of cyber-attacks in IEEE 9-bus system that may have objectives in the framework of cyber physical studies. The results will quantify the cyber-attacks that relate to the requirement of detection and mitigation in the distribution/transmission network. In other words, with estimates on critical/threshold, one can identify beyond which, detection and mitigation cannot be performed at the time of cyber-attacks in the system.

Scope:
The study is limited to transmission network and analysis is performed

Following experiments/activities were planned to achieve the above-specified objectives:
Test 1 (T1): Change in active power load
Test 2 (T2): Change in reactive power load
Test 3 (T3): Change in inertia (emulates integration of renewable resources in the grid energy)
Test 4 (T4): Impact of various sliding surface and circuit breaker status
The above tests (case studies) were planned for typical changes in active and reactive power load (operating conditions of power network) and inertia changes that emulates to reduction in system inertia on integration of renewable energy. Also, study on different sliding surfaces and point of attack were included.

1.3 Structure of the Document

This document is organized as follows: Section 2 briefly outlines the state-of-the-art/state-of-technology that provides the basis of the realized Lab Access (LA) User Project (UP). Section 3 briefly outlines the performed experiments, whereas Section 4 summarises the results and conclusions. Potential open issues and suggestions for improvements are discussed in Section 5. Finally, additional information is provided in Appendix A.

2 State-of-the-Art/State-of-Technology

The coordinated switching attack is an intelligent cyber-physical attack technique in which the intruder reconstructs system trajectory based on variable structure theory [1]. The vulnerability analysis is also investigated for coordinated variable structure switching on various systems. In this attacking scheme, the intruder gains control over a target switch and applies a variable structure switching attack to destabilize the system [2]. Further, the performance of imperfect attack is evaluated for local system dynamics and partial knowledge of the generator state. In this approach, the intruder employs the Luenberger-based state estimation technique [3]. There is the possibility of a progressive switching attack with the application of two or more switches in conjunction with each other. It provides an auxiliary extent of freedom for an intruder to impel cascaded and coordinated switching attacks in the power system. [4], [5]. The variable structure system theory is employed to demonstrate and singularize the interconnectivity of cyber-physical systems and information of systems available to an intruder. The objective of an intruder is to apply a coordinated switching sequence to distrust the normal operation of the system in a minimum interval of time. Destabilization of the targeted generator is realizable through data corruption and communication network interruption with state-dependent circuit breaker switching [6]. The linear sliding surface exhibit chattering due to inherent circuit breaker delays and hysteresis. Therefore, a non-linear sliding surface can be imposed to devise a switching sequence. The intruder can also utilize the basic swing equation to devise the stable boundary limit for the target generator and perpetrate an attack by gaining access [2].

The existing literatures fail to provide framework about cyber-attack construction that can lead to instability in the transmission network. On account of this, study documented here highlights the situations under which generator can become unstable at the time of cyber-attack for different cases.

3 Executed Tests and Experiments

3.1 Test Plan, Standards, Procedures, and Methodology

The switching sliding mode based cyber-attack algorithm was implemented on IEEE 9-bus system, in a view to change the status of circuit breaker and/or relay on the lines in the network using RTDS Simulator. The RTDS Simulator is used as a crucial component of cyber security testbeds, in which simulated power system can be connected to real protection, control, and measurement equipment and subjected to both intentional and unintentional attacks. This provides a realistic, flexible and contained environment for validation of energy system security technologies [https://www.rtds.com/application/cybersecurity]. The complete study was carried on test bed, with interfacing of MATLAB and RTDS. The interfacing of MATLAB and RTDS was established via a TCP connection with the help of TCP protocol, i.e., ListenOnPort() command.

Test Plan	Activities
Pre-visit	Discussion with host institute/laboratory and preparation of test-bed
1st week	Integration of components (hardware and software) to establish the required test bed
2nd week	Conduct test for the successful running of test bed (IEEE 9-bus model in RSCAD and switching logic/algorithm in MATLAB)

3rd week	Interfacing of RSCAD and MATLAB via communication protocol
4th week	Successful imitation of intruder

It was assumed that intruder has some partial information about system dynamics, via PMU data, on the basis of which, intruder designs sliding surface s(x) for attack construction. The communication channel provides protocol suite to communicate between RTDS and MATLAB (run on different computer).The most widely used protocol suite is transmission control protocol/Internet protocol (TCP/IP) because of its higher speed over ethernet and minimum/lower error during data transmission. Various cyber-intrusion techniques can be used to to get access of TCP/IP layer. The constructed attack algorithm falsify the status of circuit breaker based on proposed logic/algorithm. Fig. 2 illustrates the attack algorithm and its exection on power network.

The logic/algorithm was constructed in such a manner that circuit breaker remains connected if switching logic remained satisfied otherwise circuit breaker gets disconnected. But the start-time and stop-time of logic implementation depends on trajectory derived from overlapping phase-portarit of power system network. Overlapping phase-portarit is nothing but the plot of rotor angle and rotor speed of generator for both condition i.e. when circuit breaker(s) is(are) connected and disconnected. Therefore, the attack algorithm changes the status of circuit breaker till stop time gets deactived and hence, trajectory of system also changes and causes large deviation in system variabls i.e. δ and ω. The large deviation in system makes system dynamics unstable and intruder becomes successful in attack implementation.

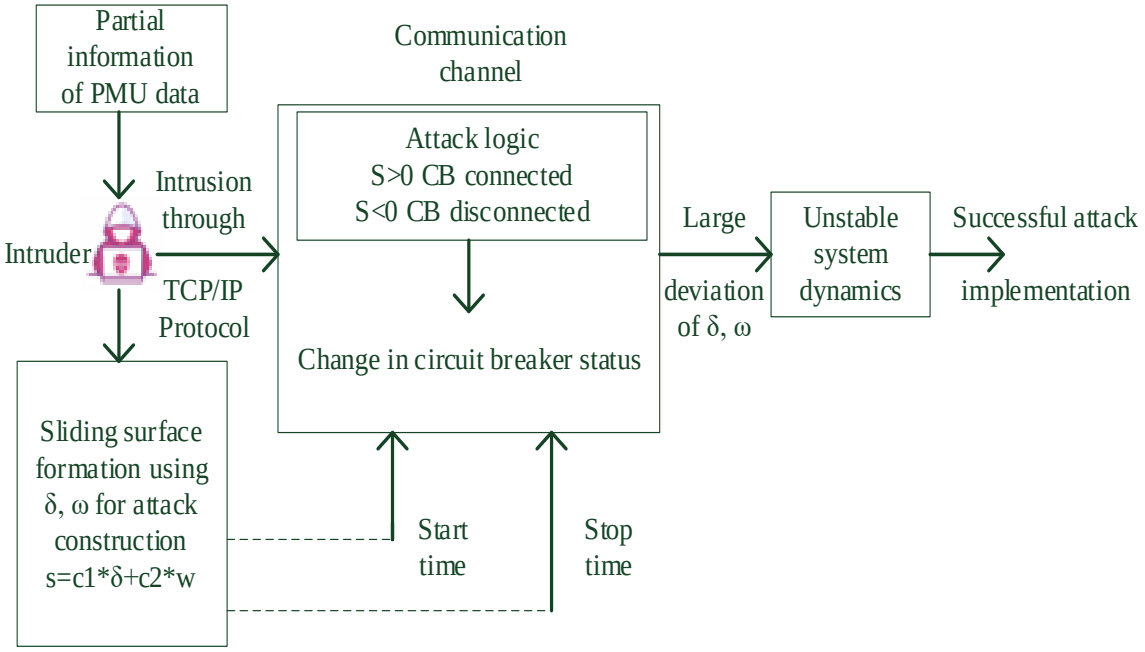


Figure 3 Block diagram of switching-sliding mode attack

3.2 Test Set-up(s)

The proposed switching sliding mode attack construction is implemented on standard IEEE 9-bus system (reduced equivalent of the Western System Coordinating Council system). Figure 4 shows the one-line diagram of these test systems. The power flow and dynamic data pertaining to the test system can be referred from RSCAD manual and given in Table 1[8]. The standard IEEE 9-Bus model can be accessed in RSCAD.

Table 1: Power flow data of test system

BUS	Type	V (pu)	PG (MW)	QG (MVAr)	PL (MW)	QL (MVAr)	H (sec)
1	SLACK	1.040∠0.0	71.6	27.0	-	-	23.64
2	P-V	1.025∠9.3	163.0	163.0	-	-	6.40
3	P-V	1.025∠4.7	85.0	85.0	-	-	3.01
4	P-Q	1.026∠-2.2	-	-	-	-	-
5	P-Q	0.996∠-4.0	-	-	125.0	50.0	-
6	P-Q	1.013∠-3.7	-	-	90.0	30.0	-
7	P-Q	1.026∠3.7	-	-	-	-	-
8	P-Q	1.016∠0.7	-	-	100.0	35.0	-
9	P-Q	1.032∠2.0	-	-	-	-	-

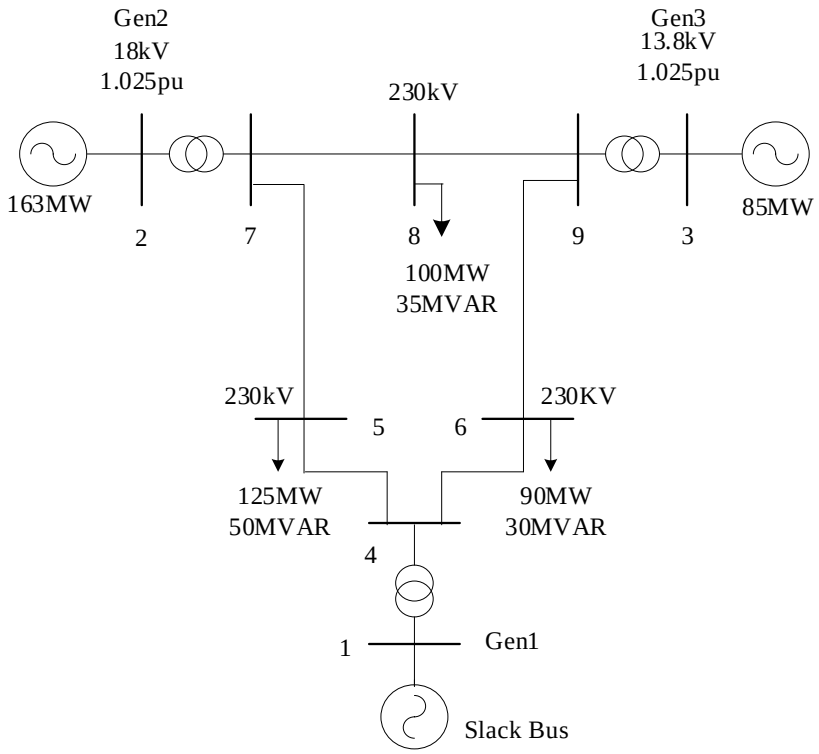
The strategy of switching attacks was applied through the MATLAB platform. The strategy includes:

1. Design of stable sliding surface S(x) following Lyapunov theorem: Sliding surface directs the trajectory of the system in the desired manner
2. Switching of circuit breaker: The circuit breaker operates according to the given logic.

$$S(x) > 0, Circuit\ breaker\ activated$$

$$S(x) < 0, Circuit\ breaker\ deactivated$$

The interfacing of RSCAD/RTDS and MATLAB (or any external program) as shown in Fig. 4 can be implemented through TCP/IP socket communication. The ListenOnPort() Command establishes TCP/IP socket communication with an interaction speed limit of up to hundreds of milliseconds. When command ListenOnPort() is executed, RSCAD/Runtime starts acting like a socket server, whereas MATLAB acts like a socket client. Once the TCP socket is established, it can be considered as a pipeline where the RSCAD/Runtime script command can be fed at one end and taken out at the other end. The MATLAB platform feeds attack algorithm into the pipeline, while RSCAD/Runtime receives the attack algorithm and changes the status of the circuit breaker in the test systems.



(i) IEEE 9-bus system

Figure 4 One-line diagram of test systems

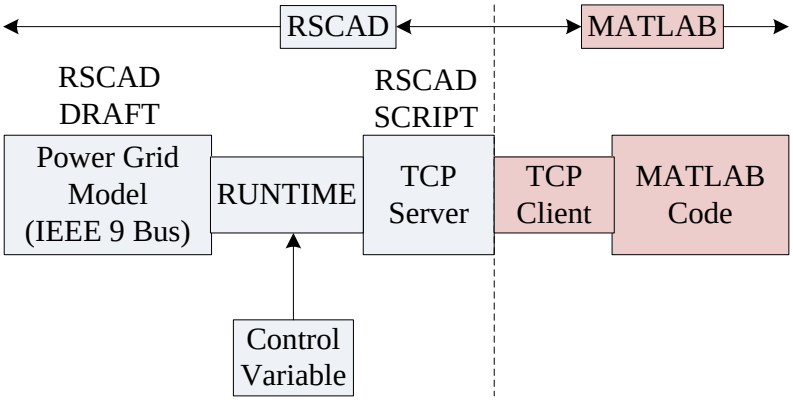


Figure 5 Interfacing of RSCAD/RTDS with MATLAB

The different test cases performed are given in followings sub-sections:

3.2.1 Test 1.1 configuration

This test case is carried out for changes in active power load in the network as given in Table 1.

Table 1: P_L change, Q_L Nominal, CB-4 operating for IEEE 9-bus system

S.No.	L5 (MW)	L6 (MW)	L8 (MW)
Case 1(A)	125	90	200

Case 1(B)	125	90	75
Case 2(A)	100	90	200
Case 2(B)	100	45	200
Case 2(C)	50	45	200
Case 3(A)	75	90	200
Case 3(B)	75	45	200

3.2.2 Test 1.2 configuration

This test case is carried out for changes in reactive power load in the network as given in Table 2.

Table 2: P_L change, Q_L Nominal, CB-4 operating for IEEE 9-bus system

S.No.	L5 (MVAr)	L6 (MVAr)	L8 (MVAr)
Case 1(A)	50	30	45
Case 1(B)	50	30	25
Case 2(A)	40	30	45
Case 2(B)	60	30	45
Case 3(A)	40	20	45
Case 3(B)	40	15	45
Case 4(A)	25	30	45
Case 4(b)	25	15	45

3.2.3 Test 1.3 configuration

This test case is carried out for changes in system inertia in the network as given in Table 3.

Table 3: Change in system inertia for IEEE 9-bus system

S.No.	H1(sec)	H2(sec)	H3(sec)
Case 1(A)	18.91	6.4	3.01
Case 1(B)	11.82	6.4	3.01
Case 2(A)	23.64	5.12	3.01
Case 2(B)	23.64	3.2	3.01
Case 3(A)	23.64	6.4	2.408

3.3 Data Management and Processing

The results obtained from Real Time Digital Simulator are stored in a DAT file. The DAT file is a data file that contains information about the result, which has been stored and further analyzed. The DAT file can be accessed using RSCAD, MATLAB, and using any text editor like

Notepad. The user has extracted and analyzed the DAT file using MATLAB. MATLAB provides freedom to plot the results among different data available (i.e., Rotor angle difference, Rotor speed, sliding surface, etc.).

4 Results and Conclusions

4.1 Discussion of Results

The IEEE 9-Bus power system model is available in draft section of RSCAD. The implementation of switching-sliding mode attack requires control of circuit breaker, in order that some modifications have made in the draft model with aid of control system library. The control system library allows customised control system to be created that can interact with the model power system and/ or the outside world. The modifications in standard model incorporates: controllable circuit breaker with 6 switches corresponding each circuit breaker.

The RSCAD/Runtime offers a script function for automating the operation of the RTDS simulator. The script function can be used for interfacing MATLAB and RTDS using TCP/IP socket communication. The TCP/IP socket communication can be establish with “ListenOnPort()” command. The ListenOnPort script command provides a way for an external process (MATLAB) to control RSCAD by sending regular script commands over a TCP/IP connection.

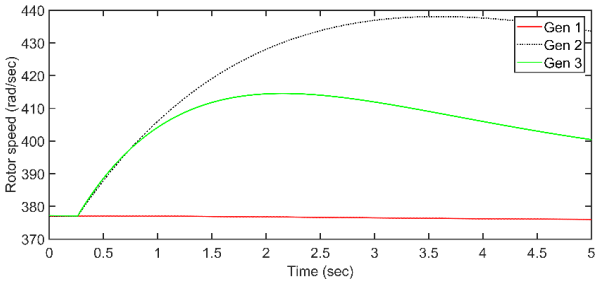
Syntax: ListenOnPort(int portNumber);

MATLAB is a programming and numeric computing platform applied to imitate the intruder and develop an attack algorithm. The sliding surface S(x) is designed based on Lyapunov theory and further attack algorithm is designed based on sliding surface S(x). The MATLAB script involves code for establishing TCP/IP socket communication, fetching external variable (rotor angle and rotor speed of generator) and implementing attack algorithm. The script file of MATLAB will fetch external variable continuously and compare with attack algorithm. If attack algorithm satisfies the MATLAB will send command to RSCAD to change the status of circuit breaker. This operation will initiate and terminate at ‘Start Time’ & ‘Stop Time’ consequently. The start and stop time is identified with aid of phase-portrait (graphical representation of rotor angle vs rotor speed of generator) of system. The Stop time is the time at which the phase-portrait or trajectory of system diverge towards infinity (system will go to instability) and the Start time is identified as time, which requires minimum time to reach at stop time and minimum switching will take between this process. The sliding surface impart a direction to system trajectory towards infinity.

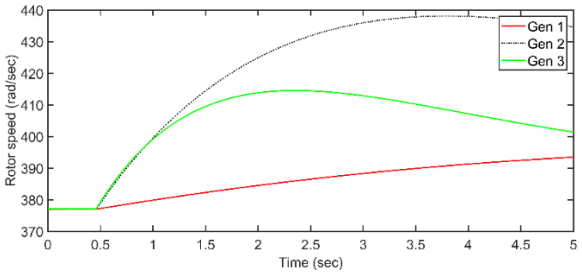
4.1.1 Test 1.1 configuration

The test case 1.1, is carried out for changes in active power load in the network. The sliding surface selected for this case $S1 = 5\delta - 0.005\omega$ and $S2 = 0.0095\delta - \Delta\omega$ are applied corresponding circuit breaker CBR_57 and circuit breaker CBR_79 at start time= 0.01sec and stop time= 0.5sec for CBR_57, the start time= 3.2sec and stop time= 4.0sec for CBR_79.The CBR_57 is operated remotely according to sliding surface S1 and CBR_79 is operated remotely according to sliding surface S2. The rotor speed of generator gradually increases and violate the frequency stability criterion as shown in Figure 6(a). The variation of frequency for generator 2, is more than rated ±5% represents successful implementation of switching-sliding mode attack construction. The active power load is reduced in Case 1(b) at Load L8 causing power imbalance and more frequency variation in Generator 2 and 3. Similarly, active power is varied at different load including load L5, L6 and L8. The frequency of most effected generator is varied (either

positive or negative) with respect to change in active power and can be verified through Figure 6(a), 6(b), 7(a), 7(b), 7(c),8 (a) and Figure 8(b).

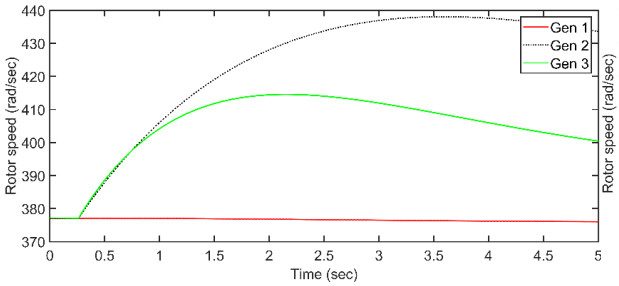


(a) Case 1(A)

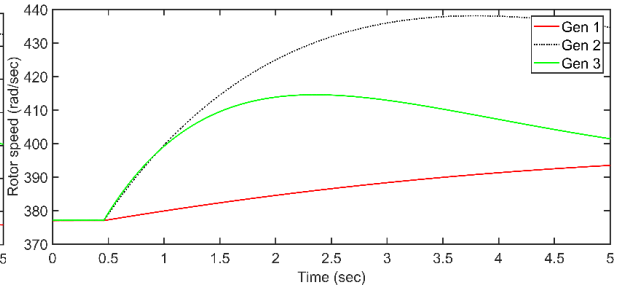


(b) Case 1(B)

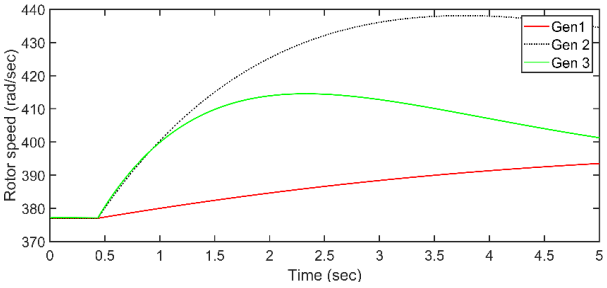
Figure 6 State variable for Test 1.1



(a) Case 2(A)

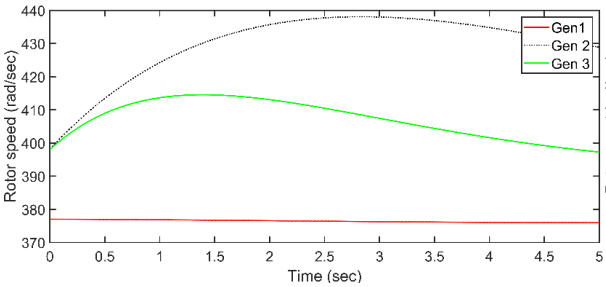


(b) Case 2(B)

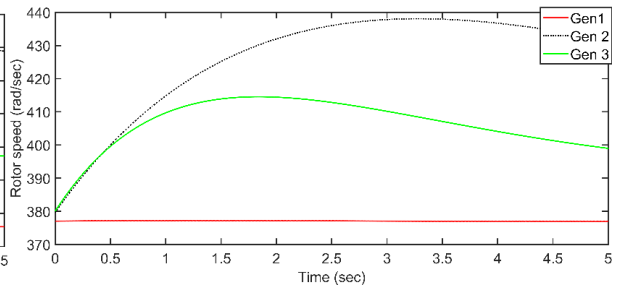


(b) Case 2(C)

Figure 7 State variable for Test 1.1



(a) Case 3(A)

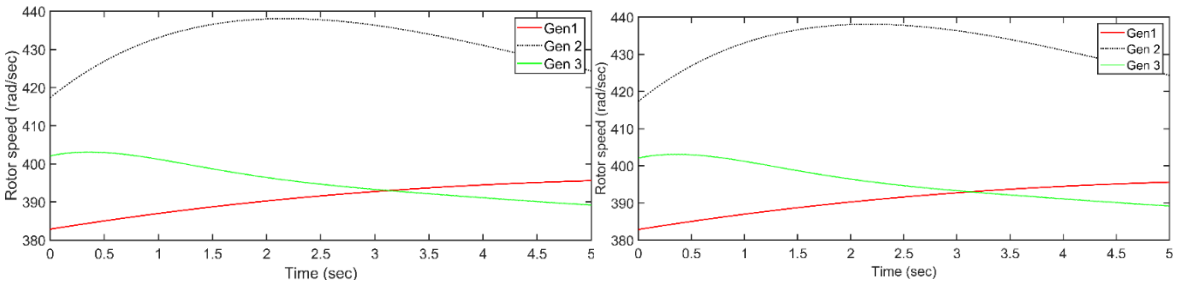


(b) Case 3(B)

Figure 8 State variable for Test 1.1

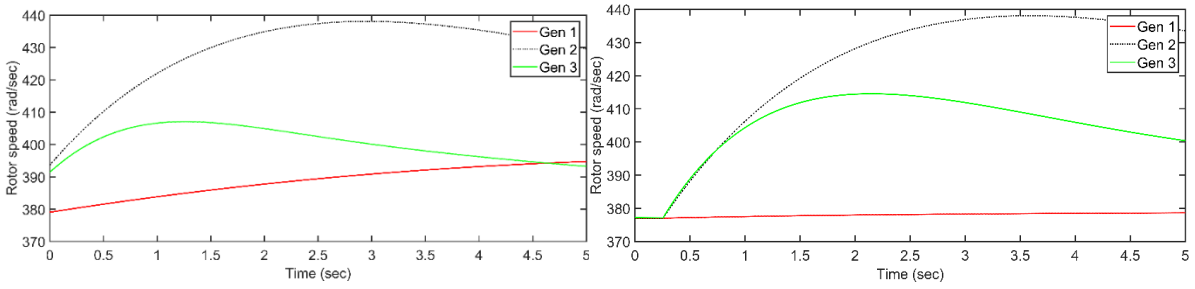
4.1.2 Test 1.2 configuration

The test case 1.2, is carried out for changes in reactive power load in the network. The sliding surface selected for this case $S1 = 5\delta - 0.005\omega$ and $S2 = 0.0095\delta - \Delta\omega$ are applied corresponding circuit breaker CBR_57 and circuit breaker CBR_79 at start time= 0.01sec and stop time= 0.5sec for CBR_57, the start time= 3.2sec and stop time= 4.0sec for CBR_79.The CBR_57 is operated remotely according to sliding surface S1 and CBR_79 is operated remotely according to sliding surface S2. The rotor speed of generator gradually increases and violate the frequency stability criterion as shown in Figure 9(a). The variation of frequency for generator 2, is more than rated ±5% represents successful implementation of switching-sliding mode attack construction. The reactive power load is reduced in Case 1(b) at Load L8 causing power imbalance and some indirect (dependent) frequency variation in Generator 2 and 3. Similarly, reactive power is varied at different load including load L5, L6 and L8. The frequency of most effected generator is loosely dependent on (either positive or negative) reactive power and can be verified through Figure 9(a), 9(b), 10(a), 10(b), 11(a), 11(b), 12(a) and Figure 12(b).



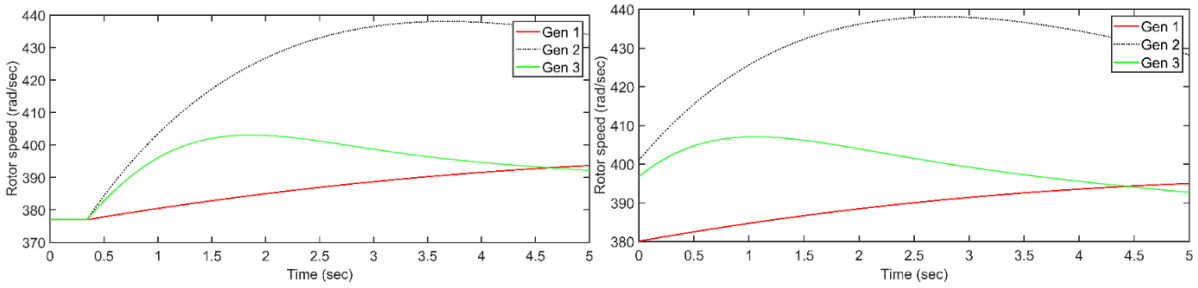
(a) Case 1(A) (b) Case 1(B)

Figure 9 State variable for Test 1.2



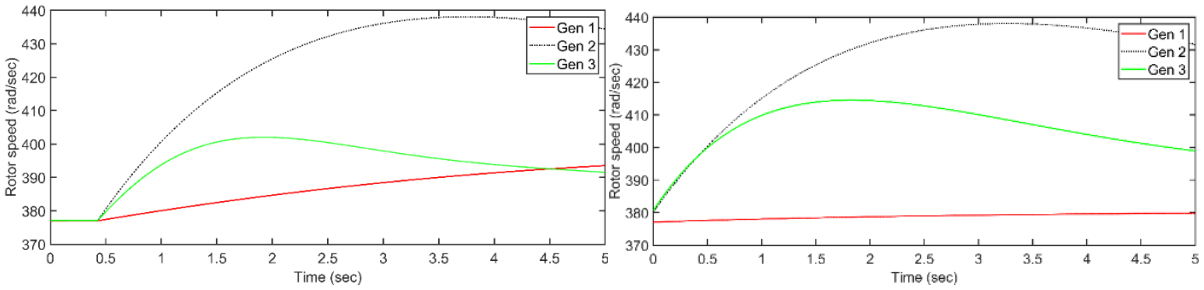
(a) Case 2(A) (b) Case 2(B)

Figure 10 State variable for Test 1.2



(a) Case 3(A) (b) Case 3(B)

Figure 11 State variable for Test 1.2

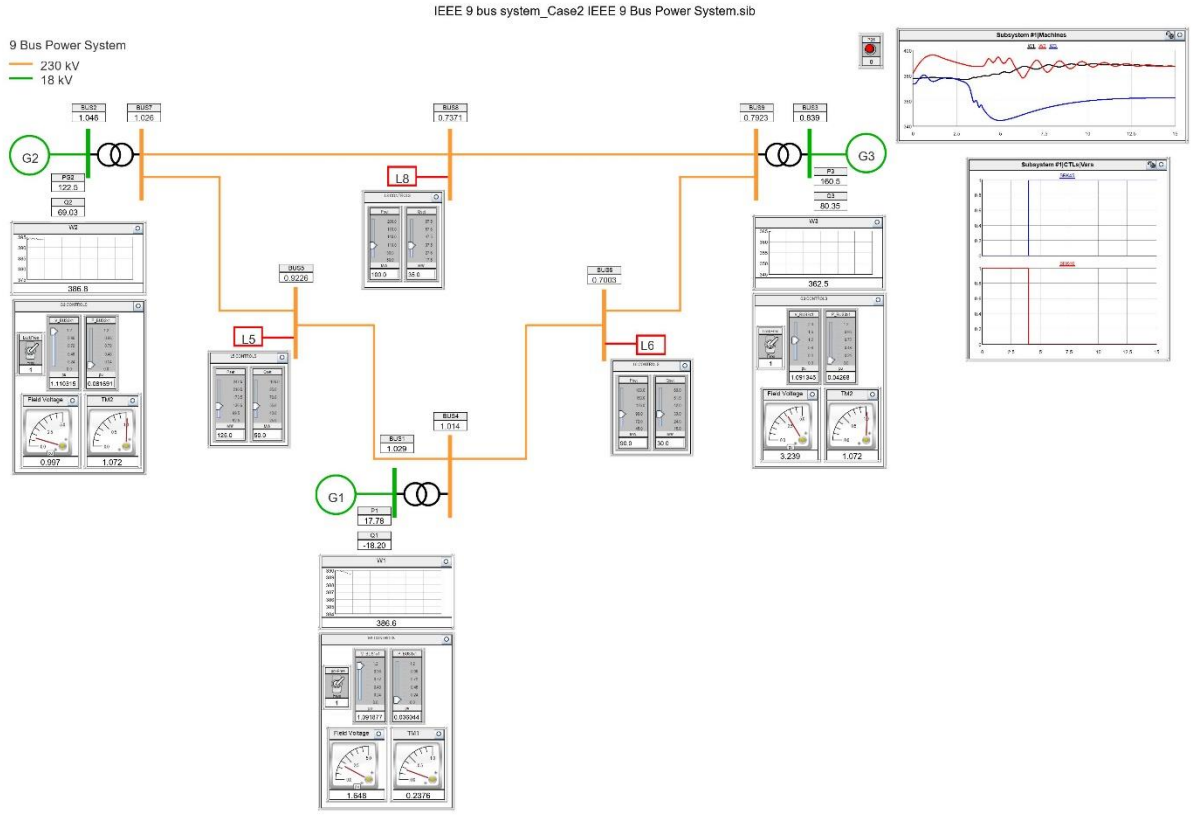


(a) Case 4(A) (b) Case 4(B)

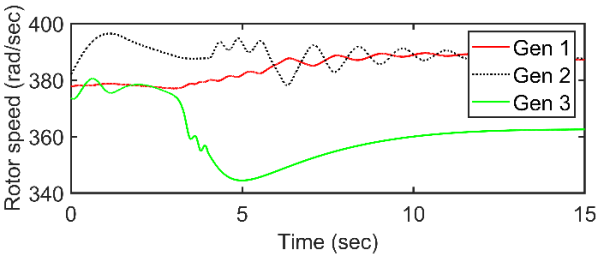
Figure 12 State variable for Test 1.2

4.1.3 Test 1.3 configuration

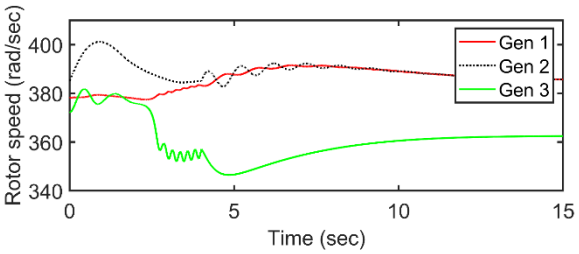
The test case 1.3, is carried out for changes in moment of inertia in generators of power ssytem network. The sliding surface selected for this case $S1 = 5\delta - 0.005\omega$ and $S2 = 0.0095\delta - \Delta\omega$ are applied corresponding circuit breaker CBR_57 and circuit breaker CBR_79 at start time= 0.01sec and stop time= 0.5sec for CBR_57, the start time= 3.2sec and stop time= 4.0sec for CBR_79.The CBR_57 is operated remotely according to sliding surface S1 and CBR_79 is operated remotely according to sliding surface S2. The rotor speed of generator gradually increases and violate the frequency stability criterion as shown in Figure 13(a). The variation of moment of inertia is considered to show integration of conventional energy resources with renewable energy resources. The change of frequency with variation of moment of inertia shown in Figure 13(a,b,c) , Figure 14(a,b) and Figure 15(c).



(a) Runtime module for Test 1.3

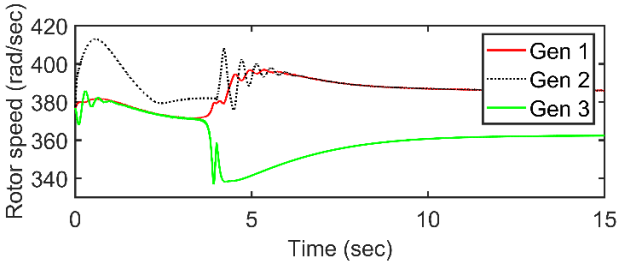


(b) Case 1(A)

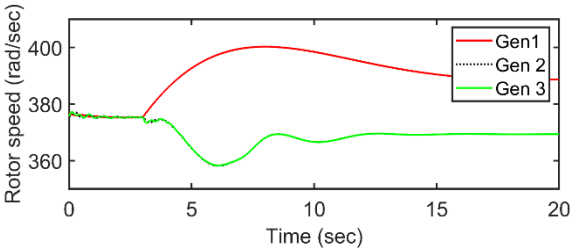


(c) Case 1(B)

Figure 13 State variable for Test 1.3

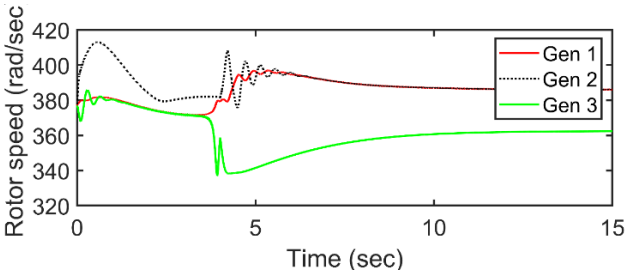


(a) Case 2(A)



(b) Case 2(B)

Figure 14 State variable for Test 1.3



(a) Case 3(A)

Figure 15 State variable for Test 1.3

4.2 Conclusions

With the opportunity available via ERIGrid 2.0 Lab Access programme, the user group have explored and demonstrated the feasibility of attack construction algorithm in real-time platform. The study and analysis via switching sliding surface for cyber-attack provided a new dimension to attack construction design based on variable structure theory. The study suggested that the switching sliding mode attack is highly dependent on initial operating condition of the power system, in terms of active power load, while loosely depends on reactive power component of the load. The use of said approach for attack construction can lead to instability in the system just by changing the status of few signals of power system network. The type of sliding surface, choice of circuit breaker, choice of attack source; all these constraints are related to implementation of successful attack. But, once the system trajectory starts to follow sliding surface with attack algorithm, the response becomes independent of system constraints.

The results and its analysis out of this study can be helpful to understand the situations/threats that may arise out of attack designed via sliding mode control theory.

The interfacing of RTDS/RSCAD and MATLAB describes the possibility of successful attack

implementation through TCP/IP communication. While, the RTDS claims that it provides real-time behaviour of test system. But due to interfacing:

1) We need to compromise between time-delay and data packet loss. The increase in sampling step reduces time delay between data packet received from MATLAB and RTDS. And further when we decrease the sampling step, then communication/interfacing time delay increases.

The addition of distributed energy resource system in conventional power system will make system more vulnerable for any type of cyber-attacks. As such, real-time study via HIL seems feasible platform wherein, related analysis can be performed/tested via attack construction algorithms. The switching sliding mode attack provides a vivid idea of attack construction as well as sufficient level of useful information towards attack detection approach. The switching response of circuit breaker is highly non-uniform and non-periodic. So, a detector algorithm can be designed to detect switching instant of circuit breaker.

5 Open Issues and Suggestions for Improvements

As a part of study during the visit, researchers could chose only one circuit breaker as source point of attack for real-time analysis. This is due to fact, that several cases for given circuit breaker was planned. However, the switching sliding mode attack provides further opportunity to implement attack at different points; circuit breaker, relay, busbar, near end of generator, load and line switching.
It was planned to apply IEC 61850 for analysis. But some more communication infrastructure/protocols can be possible to implement in real-time scenario and analyse the impact of attack. This is important, since renewable integration and its operation in smart grid environment can be expected from different protocols of communication network. The existing lab facilities can be extended to suit some of available communication networks, in addition of real-life renewable resources integration to RTDS via power hardware in loop simulation.

References

1) *Magdi S. Mahmoud, in Advanced Control Design with Application to Electromechanical Systems, 2018.*
2) *S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in 2011 IEEE 1st International Workshop on Smart Grid Modeling and Simulation, SGMS 2011, 2011, pp. 49–54. doi: 10.1109/SGMS.2011.6089026.*
3) *IEEE Staff and IEEE Staff, 2012 IEEE Power and Energy Society General Meeting.*
4) *S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated variable structure switching attack in the presence of model error and state estimation," in 2012 IEEE 3rd International Conference on Smart Grid Communications, SmartGridComm 2012, 2012, pp. 318–323. doi: 10.1109/SmartGridComm.2012.6486003.*
5) *S. Liu, B. Chen, D. Kundur, T. Zourntos, and K. Butler-Purry, "Progressive switching attacks for instigating cascading failures in smart grid," 2013. doi: 10.1109/PESMG.2013.6672314.*
6) *S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," IEEE Trans Emerg Top Comput, vol. 1, no. 2, pp. 273–285, Dec. 2013, doi: 10.1109/TETC.2013.2296440.*
7) *S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," IEEE Trans Smart Grid vol. 5, no. 3, pp. 1183–1195, 2014, doi: 10.1109/TSG.2014.2302476.*
8) *P.W. Sauer and M.A. Pai, "Power System Dynamics and Stability," IEEE Press. 1998.*

Appendix A. Script to Import external variable and Interfacing using RSCAD

```
/*
************************************************************************
********
      Import External Variable Arrays using RSCADs ListenOnPort Fea-
ture

      Script Developed By:  Christian Jegues
                          Date:   2014-10-10
                       Revised:   2022-06-13
            Original Author: Based on ListenOnPort.scr by Dr. In-Kwon
Park

                  Description:    This script is used to accommodate
the MATLAB
                                        script importExternVarLOP.m
used to import
                                        external variables from RSCAD
to MATLAB.

         Additional Notes: N/A
************************************************************************
********
*/
//**********************************************************************
********
//    External Variables:
//**********************************************************************
********

external "Subsystem #1 : Machines : BUS1x1 : RA1"RA1;
external "Subsystem #1 : Machines : BUS1x1 : W1"W1;



//**********************************************************************
********
//    Local Variables:
//**********************************************************************
********
float myArrayValues;
int myArraySize;
string temp_string; // For token string generated from Runtime

float myArrayValues2;
int myArraySize2;
string temp_string2; // For token string generated from Runtime

//**********************************************************************
********
```

```
//    Main Program:
//*****************************************************************
********
fprintf(stdmsg, "Runtime is now acting as TCP Server...\n");

ListenOnPort(4575, true);

fprintf(stdmsg, "Runtime is now finished acting as TCP S
```

Disclaimer

This document contains material, which is copyrighted by the authors and may not be reproduced or copied without permission.

The commercial use of any information in this document may require a licence from the proprietor of that information.

Neither the Lab Access User Group as a whole, nor any single person warrant that the information contained in this document is capable of use, nor that the use of such information is free from risk. Neither the Lab Access User Group as a whole, nor any single person accepts any liability for loss or damage suffered by any person using the information.

This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of its content.

Copyright Notice

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 870620.