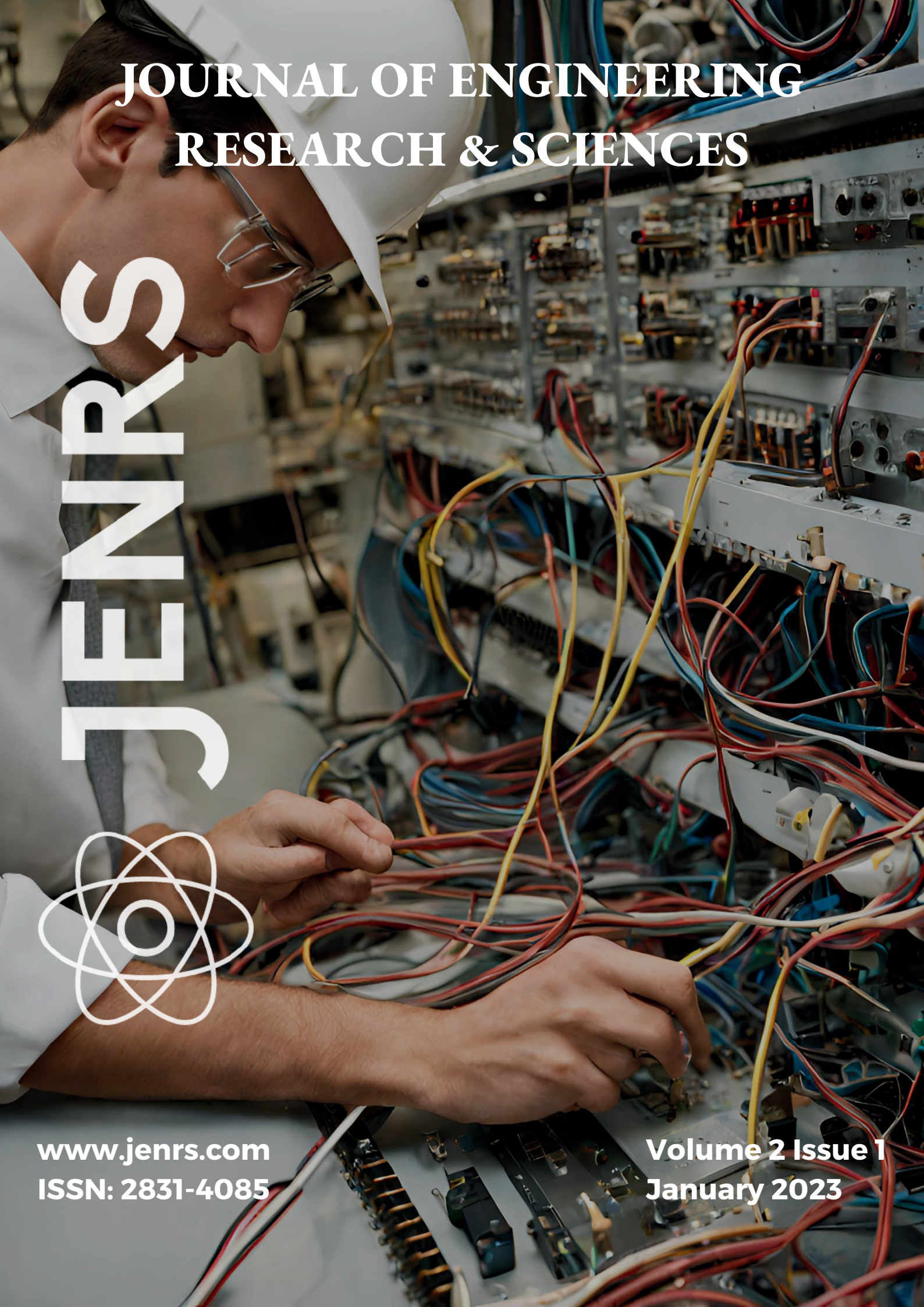
JOURNAL OF ENGINEERING RESEARCH & SCIENCES

JENRS



www.jenrs.com
ISSN: 2831-4085

Volume 2 Issue 1
January 2023

EDITORIAL BOARD

Editor-in-Chief

Editorial Board Members

Editorial

The current edition of our journal showcases three groundbreaking research papers that push the boundaries of technology and engineering. These studies span diverse fields, including power system stability, mobile application security, and 5G communication technologies. Each paper not only presents innovative solutions but also lays the groundwork for future research and development in their respective areas.

The first paper delves into the critical realm of automatic generator control (AGC) within the National Transmission System (NTG). Focused on the Baba Hydroelectric Power Plant in Ecuador, this research offers a comprehensive examination of the oscillations in generator control systems and proposes robust solutions. By meticulously tuning both the Automatic Voltage Regulator (AVR) and the Power System Stabilizer (PSS), the authors have developed a model that adapts to various operating conditions. Their findings underscore the importance of a high-gain AVR for steady state and transient stability while highlighting the PSS's role in mitigating oscillatory instabilities. This study's validation strategy, employing the average quadratic mean square error method, provides a reliable framework for future enhancements in power system stability [1].

In an era where mobile applications are integral to daily life, ensuring the security of user information is paramount. The second paper addresses this pressing need by introducing CAPEF, a context-aware policy enforcement framework designed for Android applications. This innovative system mitigates privacy leakage by enforcing inter-app security policies without altering the underlying platform. The research demonstrates CAPEF's effectiveness through rigorous experimentation, showcasing minimal impact on application size and execution time even as policy complexity increases. By preventing malware collusion and safeguarding sensitive user information, CAPEF represents a significant leap forward in mobile application security [2].

The third paper presents a novel approach to designing a bandpass filter using substrate integrated waveguide (SIW) topology for 5G applications. This research aims to produce a dual-mode passband characteristic with a wide upper stopband behavior centered at 4.7 GHz. By incorporating Stepped Impedance Resonator (SIR) slots and E-shaped resonator slots, the authors have achieved remarkable improvements in selectivity and stopband response. The addition of surface mount varactor diodes enables tunable characteristics, allowing the center frequency of the passband to be adjusted over a range of 600 MHz. The successful fabrication and verification of the developed filter underscore its potential impact on advancing 5G communication technologies [3].

These three papers exemplify the cutting-edge research and innovative solutions that define our journal. From enhancing power system stability to securing mobile applications and pioneering 5G technologies, the contributions of these studies are both profound and far-reaching. We are proud to present these works to our readers and look forward to the continued advancements they will inspire in their respective fields.

References:

[1] J. Urquizo, D. Bonilla, F. Rivera, R. Chang, “Modelling, Simulation and Sensitivity Analysis of Generator Control Systems using Coexisting and Cooperative Tools,” Journal of Engineering Research and Sciences, vol. 2, no. 1, pp. 1–12, 2022, doi:10.55708/js0201001.

[2] S. Inshi, M. Elarbi, R. Chowdhury, H. Ould-Slimane, C. Talhi, “CAPEF: Context-Aware Policy Enforcement Framework for Android Applications,” Journal of Engineering Research and Sciences, vol. 2, no. 1, pp. 13–23, 2022, doi:10.55708/js0201002.

[3] Md.A. Rahman, P. Sarkar, “A Tunable Dual-mode SIW Cavity Based Bandpass Filter with Wide Upper Stopband Characteristics,” Journal of Engineering Research and Sciences, vol. 2, no. 1, pp. 24–29, 2022, doi:10.55708/js0201003.

Editor-in-chief

Prof. Paul Andrew

JOURNAL OF ENGINEERING RESEARCH AND SCIENCES

Volume 2 Issue 1 January 2023

CONTENTS

Received: 28 October, 2022, Revised: 11 December 2022, Accepted: 18 December, 2022, Online: 28 January, 2023

DOI: https://dx.doi.org/10.55708/js0201001

Modelling, Simulation and Sensitivity Analysis of Generator Control Systems using Coexisting and Cooperative Tools

Javier Urquizo[1,*], Diover Bonilla[1], Francisco Rivera[1], Rommel Chang[2]

[1]Escuela Superior Politécnica del Litoral, ESPOL, FIEC, Campus Gustavo Galindo Km. 30.5 Via Perimetral, Guayaquil, Ecuador
[2]CELEC EP Unidad de Negocio Hidronación, Central Baba, Kilómetro 39 vía Quevedo -- Santo Domingo, Ecuador
*Corresponding author: Javier Urquizo, ESPOL/FIEC, Km. 30.5 Via Perimetral, +593982226142 jurquizo@espol.edu.ec

ABSTRACT: This research is about tuning the automatic generator control (AGC) unit within the National Transmission System (NTG) and is intended to provide a set of key insights into problems related to generator control systems oscillations and the possible available solutions. The case study is the Baba Hydroelectric Power Plant in Ecuador. The aim is to model, simulate and validate the controls of the Baba generating units for an optimal and stable response. Both controllers, the Automatic Voltage Regulator (AVR) and Power System Stabilizer (PSS) were tuned using both a component-based approach using an object-orientated tool where the model structure resembles the original system, and a coexisting power flow tool in a signal orientated environment. A key part of this tuning is the adaptation of the model to different operating conditions by testing scenarios where signals ought to be defined before the start of the simulation and others be chosen for visualisation without any limitation, therefore, this paper is about finding a multi-framework environment. Also, the model was disturbed so to observe the field Voltage and terminal voltage values using a simplified and reduced part of the NTG. Results show that a high gain AVR helps the steady state and transient stabilities but may reduce the oscillatory stability and the PSS can provide significant stabilization of such oscillations. The validation strategy uses the average quadratic mean square error statistical method.

KEYWORDS: Electric Power Systems, Automatic Voltage Regulator, Coexisting and Collaborative tools, Power System Stabilizer, Stability Assessment, Sensitivity Analysis

1. Introduction

Hydroelectric power plants are the foundation of Ecuador's power generation capacity. Hydropower plants account for 57.67% [1] of the country's installed capacity by 2017. Our case study is the Baba Multi-Purpose Project (BMP), consisting of four dikes and three channels in Los Ríos province, used for irrigation, flood control, water supply and hydroelectric power generation. The BMP includes water supply to the reservoir and the Daule-Peripa reservoir, construction of the hydroelectric power plant and associated transmission lines. Therefore, the main purpose of the BMPs is water storage and transmission, not hydropower. Upland rice is dominant in Los Rios and no-tillage is the dominant crop cultivation method. About 60 percent of the farmers farm less than five hectares per person and three percent are large farmers cultivating 100 hectares per person [2]. With 3,000 hectares of land at risk of flooding, protesters against the Baba dam had a major impact on the construction of the dam and saved the community from flooding [3]. Capable of generating 42 MW, covering 40-50% of the demand in Los Ríos. The Baba hydropower station has two of his Kaplan direct shaft turbines submerged by a spiral cover or scroll area.

This paper concerns the feasible enhancement controls which may allow the countrywide electricity grid to perform reliably over broader tiers of loading and system operational point. Hydro-turbines controllers are tuned for assumed situations withinside the relaxation of the electricity grid; however, as grid situations vary, the controllers eventually 'malfunction' in one-of-a-kind ways (ranging being too sluggish and/or of inadequate ability or loss of coordination) [4]; consequently, it is hard to ensure system-wide performance; therefore, the general tendency is not to rely on control outside normal regions and find

out where are the opportunities to operate efficiently. A method is wanted for dealing with the machine throughout a huge variety of running condition, for this is important to display electricity-flows and adjust those consistent with the higher described generator interconnection standards making sure viable electricity exchanges without compromising machine reliability; however, at the same time, the design has to be completed in order that every generator maintains its decentralized, self-sufficient operation, whilst coordinating with turbines of the nearby electricity grid.

Literature review shows different ways authors can implement controls. For example, Std 421.5™-2005 [5] describes a model structure intended to facilitate the use of field test data as a means of obtaining model parameters. In North America model validation is mandated according to the Reliability Council (NERC) Modelling, Data, and Analysis (MOD) series of standards. NERC MOD-033-1 [6] specifies consistent validation requirements to facilitate the collection of accurate data and the development of planning models for reliability analysis of interconnected transmission systems. In Europe, [7] designed a robust controller to address both local area and inter-area oscillations. The controller is a second-order state-space regulator. In Ecuador, [8] is developing tools for displaying oscillation modes and their damping, and for provisional localization of a PSS in the Ecuadorian NTG. An online model estimation scheme was also used to validate and/or tune a small-signal model of the power system using synchro phasor data [9] at the Paute-Molino power plant in Ecuador [10]. In Modelica [11] there was an effort on design principles and a prototype for modelling the pan-European electricity grid to be used by European transmission system operators.

The controls are an Automatic Voltage Regulator (AVR) and a Power System Stabilizer (PSS). The AVR regulates the terminal voltage of the generator. A fast-response high-gain AVR improves large-signal transient stability in the sense that it improves the network's ability to maintain synchronism when subjected to severe transient disturbances. There is a trade-off between synchronous torque provided by the AVR and the damping torque provided by the PSS [12,13]. PSS tuning is for a wide oscillation damping applications. PSS requires a reliable model of the system in a software package such as DigSILENT PowerFactory (PF). The early stages of this research involved extensive data management, cleansing, and restructuring to the NTG initial dataset in the PF package. The development of these controllers uses an object-oriented and non-causal modelling approach in which individual parts of the model are directly described as equations using a declarative approach [14] but also coexisting in good cooperation with signal-orientated tools.

2. Methodology

2.1. Generation unit modelling

The Baba power generation unit will generate 161 GWh/year by pumping water to the Santa Elena Peninsula at up to 234 m^3/sec. During the rainy season (January to October), the reservoir only provides a downstream flow of 10 - 15 m^3/sec. The generating units are two horizontal axis Kaplan turbines, each of 21 MW, with a maximum operating flow of 86 m^3/ sec. The difference from the maximum flow rate, approximate 62 m^3/sec, is discharged via a by-pass installed next to the pressure line [15]. Clarke and Park transforms are commonly used in field-oriented control of three-phase AC machines. The Clarke transform converts the time domain components of a three-phase system (in abc frame) to two components in an orthogonal stationary frame (αβ). The Power System Analysis Toolbox (PSAT) hydroelectric salient pole machine is modelled as Order V Type 2 model [16], which more closely resembles the Baba generator characteristics. Both follows Van-Cutsem and Papangelis [17] proposed data (see Figure 1). Baba generator parameters and initial NTG values are shown in Table 1. The internal parameters of the generator are the same for Isolated and in NTG operation modes, but their initialization values differ depending on the controller's mode of operation. Table 1 also shows the initial values for the Isolated - NTG generator. To view the controller's response, a voltage disturbance in the form of a pulse generator was applied to the V_{ref} input. The 'Pulse Generator' parameters are shown in Table 2.

The generation model corresponds to a three-phase synchronous generator and a classic electromechanical model with transfer functions to model the direct and quadrature inductances. Assuming an additional circuit for the direct axis, the state variables can be described as in the following equations [18]. A curious reader would have to read the GitHub repository for all the models and parameters used from the OpenIPSL library.

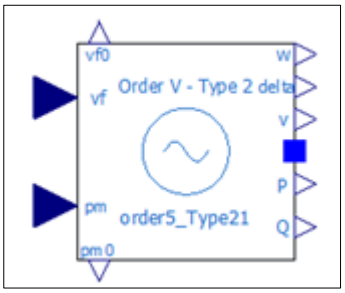


Figure 1: Machine - Generator Order V Type 2

The Model Parameters are Synchronous reactance - d axis (pu) Xd, Synchronous reactance - q axis (pu) X_q, Sub-transient reactance - d axis (pu) X_{2d}, Open circuit transient time constant - d axis (pu) T_{1d0}, Open circuit sub-transient time constant - d axis (pu) T_{2d0}, Open circuit sub-transient time constant - q axis (pu) T_{2q0}, Nominal Power (MVA) S_n,

Nominal Voltage (kV) V_n, Armature Resistance (pu) R_a, Transient Reactance - d axis (pu) X_{1d}, Mechanical inertia coefficient M and Damping D.

Table 1: Parameters of the Baba Generator

Parameter	Value	Parameter	Value
X_d	0.97	e_{1q}.start	0.950539 | 1.49748
X_q	0.78	e_{2q}.start	1.00027 | 1.47345
X_{2d}	0.29	e_{2d}.start	0 | 0.285123
X_{2q}	0.38	w.start	0 | 0
T_{1d0}	3.56	v.start	1.00027 | 0.945013
T2d0	0.028	P.start	0 | 1.88565
T2q0	0.006	Q.start	0 | 1.47173
T_{aa}	0.177	V_f. start	1.00027 | 3.125
Sn MVA	23.4	P_{m0}.start	0.900957 | 0.900957
V_n kV	13.8	p_m.start	0.900957 | 0.900957
R_a	0.0022	v_d.start	0 | 0.551147
X_{1d}	0.36	v_q.start	1.00027 | 0.76767
M	10	i_d start	0 | 2.42869
D	0	i_q.start	0 | 0.712775

Table 2: Parameters of the pulse generator

Pulse	Value
Extent	-0.03
Pulse width (%)	50
Period (s)	1
Initialization	5.65

AVR modelling is in Section 2-2 and PSS is in Section 2-3. The closed-loop response has two outputs, **P** (power) and **w** (velocity), which are connected to the corresponding inputs of the PSS. A frequency **f** block was added that allows to change the speed to frequency and therefore being able to meet the number of equations and unknowns for the Generator validation. Enhancements have also been made to the PSS output to address what-if scenarios. The internal block diagram is shown in Figure 2 and the external block diagram is shown in Figure 3.

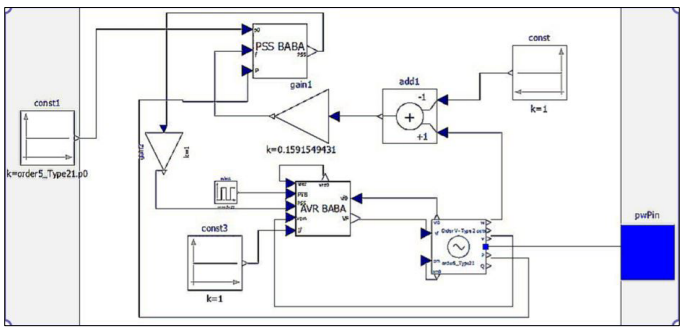


Figure 2: Baba generator internal block

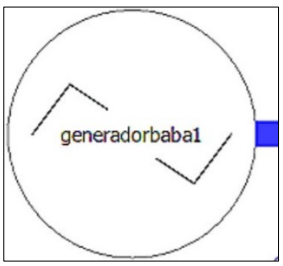


Figure 3: Baba generator external block

2.2. AVR Modelling

The IEEE 421.5 standard [5] is the IEEE recommended practice for excitation system models for power system stability studies. The models apply for frequency deviations of ±5\% from nominal frequency and oscillation frequencies up to 3 Hz. The Baba excitation system follows the IEEE 421.5 ST6B model. The AVR is shown in Figure 4 and consists of a field voltage regulator and a PI voltage regulator with a feedforward control in the inner loop. The field voltage controller implements proportional control.

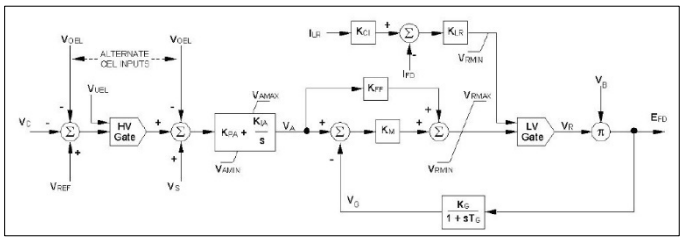


Figure 4: ST6B static potential - source excitation system with field current limiter [5]

The AVR appeared in Figure 4 comprises of a PI voltage regulator with an internal loop field voltage regulator and pre-control. The field voltage regulator executes a proportional control. The pre-control and the delay in the feedback circuit increase the dynamic response. VR represents the limits of the power rectifier. The ceiling current IFD limitation is included in this model. The power for the rectifier, VB, may be supplied from the generator terminals or from an independent source. Inputs are provided for external models of the over-excitation limiter (VOEL), under-excitation limiter (VUEL), and PSS (VS).

Baba has a static excitation system in which the generator stator voltage is rectified by a thyristor bridge. This DC excitation voltage is fed through the slip ring to the rotor windings to excite the rotor. As the energized rotor rotates within the stator, an AC voltage is generated at the stator terminals, i.e., stator voltage variations directly affect the excitation voltage. Figure 5 shows the main exciter structure underlying the exciter modelled in the simulation tool.

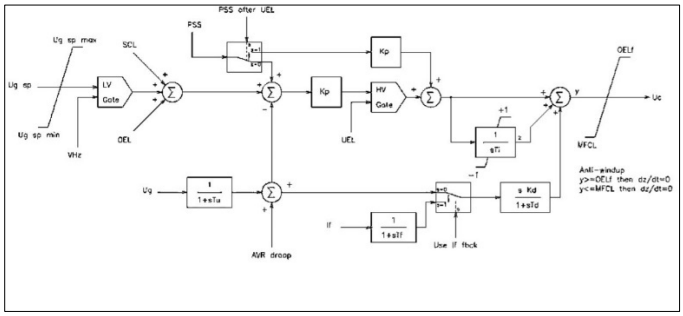


Figure 5: Excitation System, main structure [19]

The variables and parameters in Figure 5 are the maximum allowed AVR reference $U_{g\ sp\ max}$ (VHZ), the minimum allowed AVR reference $U_{g\ sp\ min}$, the transducer time constant T_u, field current time constant T_f, proportional gain K_p, integral time T_i, derivative gain K_d, derivative time constant T_d, Field current I_f, Use If the feedback in the loop control Use $I_{f\ fdbck}$, PSS after UEL, Field undercurrent limiter output MCLF, overdrive limiter output OEL, overdrive fast limiter output OEL_f, AVR compensation loop output AVR droop, Stator current limiter output SCL, Under-drive Limiter Output UEL, PSS output signal PSS, Volts hertz limiter output VHz. Typical parameter values are $U_{g\ sp\ max}$ 1.1, $U_{g\ sp\ min}$ 0.9, T_u 20 ms, T_f 20 ms, K_p 10, T_i 2 s, K_d 0, T_d 5 s, Use $I_{f\ fdbck}$ 0 (Only for brushless excitation systems), PSS after UEL 1.

Our research focuses on damping of small signal swings, so we have simplified Figure 5. It is important to model the limiter in conjunction with the voltage regulator. Under excitation limiting is especially used in turbo generators. This is because without a limiter the reactive power output from the generator could be too high, leading to erroneous simulation results. Small turbo generators connected to powerful networks are sensitive to this kind of phenomenon [20]. The purpose of the over-excited limit is to protect the generator from overheating due to prolonged field over-current.

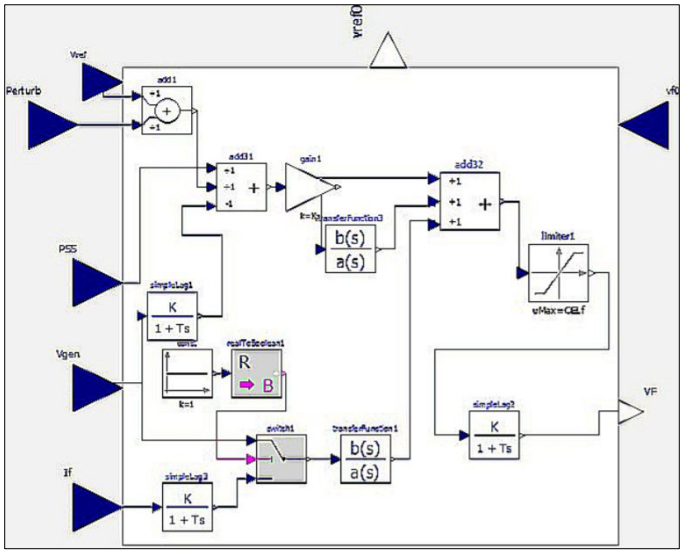


Figure 6: AVR implemented in a non-causal approach.

Figure 6 is a simplified non-causal AVR approach to modelling the Baba excitation system. Traditional approaches are based on block-oriented schemes in which causality plays a key role. However, new concepts based on object-oriented approaches, physics-oriented connections, and algebraic manipulation enable non-causal modelling, where blocks represent the interactions of equations.

Each of the transfer functions (TF) in Figure 6 has initialization parameter calibrated to stable values according to its response, either isolated or NTG modes. See Table 3.

Table 3: TF Initialization Isolated - NTG modes

Transfer Functions	Initial Isolated	Initial NTG
Simple Lag1	1.00027	0.94503
Simple Lag2	1	1
Simple Lag3	1.00027	3.12500
TransferFuntion1	0	0
TransferFuntion3	0.160044	0.499815

The AVR's operating parameters are adjusted according to a manufacturer's specified ranges and are shown in Table 4.

Table 4: Isolated and NTG AVR Parameters

Parameters	Isolated Values	NTG Values
K_p	10	10
T_i	1	2
K_d	-10	0
T_d	10	5
T_f	0.02	0.02
Tu	0.02	0.02
K_{br}	6.25	6.25
T_{br}	0.0014	0.0014
OEL_f	0.5	0.7
MFCL	-0.5	-0.5
V_0	0.75	0.7384
V_{00}	FIXED=False	FIXED=False

2.3. PSS Modelling

The IEEE 2005 421.5 standard [5] introduced a PSS structure called IEEE PSS4B. The PSS4B model represents a structure based on multiple operating frequency bands, as shown in Figure 7. Three separate bands, each dedicated to the low-, medium- and high-frequency oscillations modes, are used in the delta-omega (velocity input). Baba uses the IEEE Std 421.5™-2016 Dual-Input Power System Stabilizer (PSS_2C) [21] to improve electrical

system stability, as shown in Figure 8. A key element is the Limiter. The Limiter is used to keep the PSS output voltage within a range of values and the PSS output protection should also match the output limiter. Additional damping can be achieved to improve transient stability by setting the PSS output limit. As a result, the PSS performance improves under larger system disturbances [22].

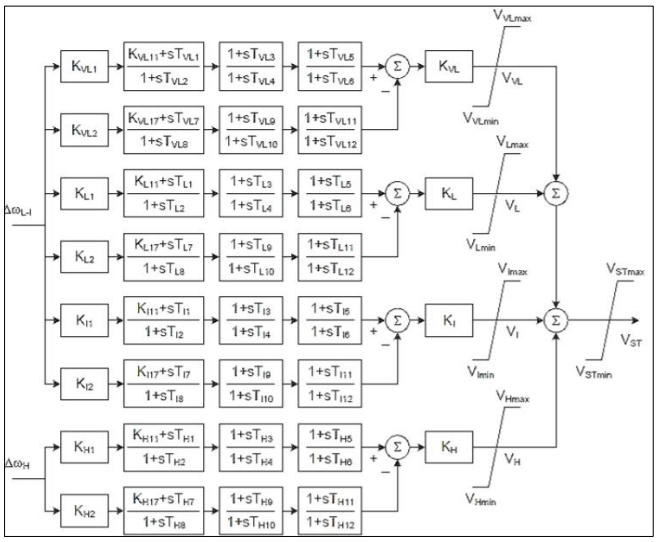


Figure 7: The multi-band stabilizer, IEEE PSS4B [5]

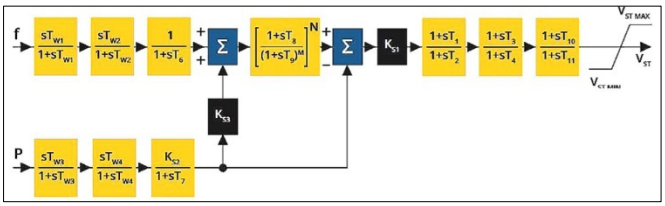


Figure 8: Power system stabilizer – PSS [21]

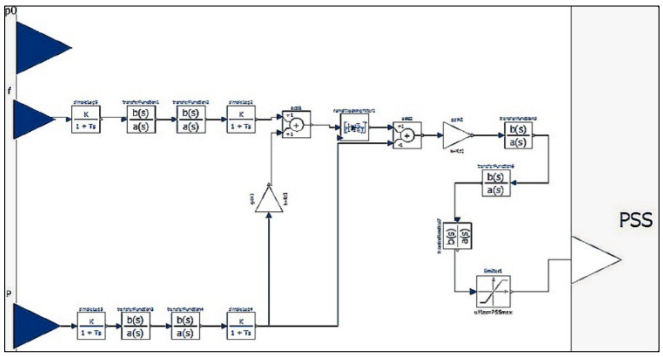


Figure 9: PSS implemented in non-causal approach.

The PSS controller has a large number of 'simple lag' and 'TransferFunction', constants, limiters, input and output signals. It also has a 'RampTrackingFilter' for attenuating the signal. Non-casual modelling is shown in Figure 9.

Each of the transfer functions (TF) of Figure 9 have initialization parameters calibrated to stable values according to their response either isolated or NTG modes. See Table 5.

Table 5: TF Initialization Isolated -- NTG modes

TF	Isolated	NTG	TF	Isolated	NTG
Simple Lag 5	0	0	Transfer Function3	0	0
Simple Lag2	0	0	Transfer Function4	0	0
Simple Lag3	0	1.87338	Transfer Function5	0	0
Simple Lag 4	0	0	Transfer Function6	0	0
Transfer Function1	0.0430175	-0,0476977	Transfer Function7	0	0
Transfer Function2	0	0			

The operating parameters of the PSS were adjusted according to the ranges specified by the manufacturer. Parameters are shown in Table 6. PSS_{min} is equal to zero.

Table 6: Isolated and NTG PSS Parameters

Parameter	Isolated	NTG	Parameter	Isolated	NTG
T_f	0.02	0.02	T_9	0.01	0.1
T_p	0.02	0.02	M	4	4
T_{w1}	3	3	N	2	1
T_{w2}	3	3	K_{s1}	0.01	0.1
T_{w3}	3	3	T_1	0.12	0.12
T_{w4}	3	3	T_2	0.03	0.03
T_6	4.6	0	T_3	0.09	0.03
T_7	3	3	T_4	0.03	0.03
K_{s2}	0.3	0.3	T_{10}	4.7	2.06
K_{s3}	1	1	T_{11}	0.37	1.3
T_8	0.2	0.4	PSS_{max}	0.05	0.05

In addition, the PSS controller is not a separate controller that is used with the generator, but it is a controller that input signals to the AVR by entering a signal into the AVR to improve the response after a failure.

2.4 National Transmission Grid

The early stages of this research involved extensive data management, cleansing, restructuring and additions to this initial dataset. In addition, real time test values of power flows were available via a robust PF power system tool. Figure 10 shows a reduced portion of the NTG with synchronous machines, transformers, transmission lines and system buses.

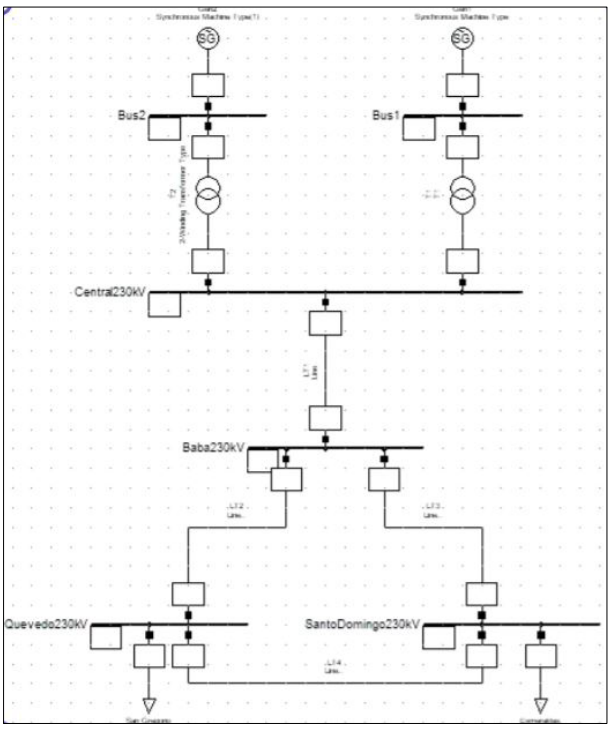


Figure 10: Reduced portion of the NTG for Baba stability studies

2.5 Transformers

Two elevating transformers (13.8:230 kV) were used for the implementation of the reduced grid. The transformer is connected to the synchronous generator. The primary winding of each transformer is connected to the generator's armature winding at 13.8 kV. A circuit breaker is installed close to transformer on the upper (230 kV) voltage side. In this arrangement any generator perturbations and grid disturbances have an effect on the transformers. Transformers implemented in our system does have serial reactance and do not have iron losses. The transformer connection is grounded wye - delta. The grounded connection will provide a path for a line-to-ground fault current (back feed current) for a fault upstream from the transformer. The parameters are shown in Table 7.

Table 7: Transformers parameters

Parameters	Values (pu)
K_T	13.8/230
x	0.5036
r	0.5

Simulation tools like PF facilitates the user with varied types of power system studies. It also obtains more detailed and accurate power-flow simulation solutions. However, the libraries integrated in the tools are normally closed for modifications. The values of power-flow that are entered in the non-causal model of transformers, generator, transmission lines and buses are acquired from PF.

2.6 Transmission Lines

A NTG transmission line is modelled with an equivalent ∏ circuit in the non-casual tool. The resistance (R) data is entered, whereas reactance (X), conductance (G) and susceptance (B) are obtained from DIgSILENT's NTG block. All values are in p.u, but the units in PF are Ω/km and need to be converted using the Zbase into per unit. Zbase is calculated from Equation 1.

$$Zbase = \frac{V^2}{P} = \frac{13{,}800^2}{46{,}760{,}000} = 4.072712\ [\Omega] \quad (1)$$

Zbase allows to compute all the lines from a reduced Baba grid. The line parameters are shown in Figure 11.

	Plant line to Baba Substation 230 Kv	Baba Substation Line to Quevedo 230 Kv	Baba Substation Line to S.Domingo 230 Kv	Line S. Domingo to Quevedo 230 Kv	Line S.Domingo to Esmeraldas 230 Kv	Line Quevedo to San Gregorio 230 Kv
R (Ω/Km)	0.101485	0.059085	0.059085	0.059085	0.05192	0.059085
X (Ω/Km)	0.49082	0.472668	0.472668	0.472668	0.4866	0.472668
Long (Km)	1.4	45	62	104	155	110
R (Ω)	0.142079	2.658825	3.66327	6.14484	8.0476	6.49935
X (Ω)	0.687148	21.27006	29.305416	49.157472	75.423	51.99348
Zbase (Ω)	4.072712					
R (pu)	0.0348856	0.6528390	0.899467	1.508783	1.975981	1.595829
X (pu)	0.1687200	5.2225793	7.195554	12.186018	18.519111	12.766305
G (pu)	28.665122	1.5317712	1.111769	0.662786	0.506078	0.626633
B (pu)	5.9269796	0.1914763	0.138975	0.082061	0.053998	0.078331

Figure11: Transmission Line Parameters

2.7 Infinite Buses

An infinite bus is the main bus of a power system with constant frequency and voltage (both in magnitude and angle). This research analyses the problem of a machine connected to an infinite bus via a transmission line. In general, fast excitation systems are usually beneficial to transient stability following large impacts by driving the field to fast response without delay. However, these abrupt changes in excitation are not necessarily beneficial in damping the oscillations that follow the first swing, and they sometimes contribute growing oscillations several seconds after the occurrence of a large disturbance [23]. We properly design the exciter as a mean of enhancing stability in the dynamic range as well as in the first few cycles after a disturbance. We consider two infinite bus implementations: the Esmeraldas and San Gregorio 230 kV buses. Input power-flow data for the non-casual system in those buses were from PF and is shown in Figure 12 for Esmeraldas as an example.

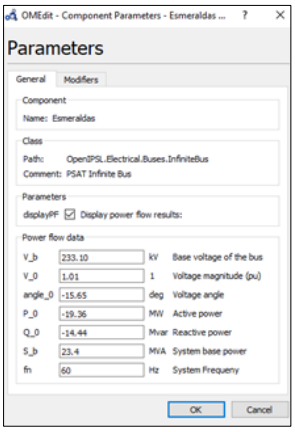


Figure 12: Esmeraldas's infinite bus parameters

2.8 Equivalent system in OpenModelica

To illustrate the effect of the excitation system on transient stability, we perform transient stability study on the equivalent system shown in Figure 13.

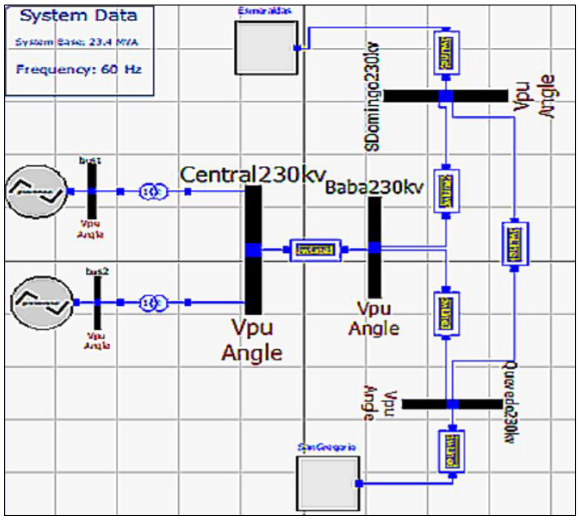


Figure 13: NTG Equivalent System

Figure 13 is the result after adding all the elements described in Sections 2.1 to 2.6. The generation parameters have been checked and AVR and PSS controller initialization values have also been adjusted as they are different from those in isolate mode.

Section 3-1 and Section 3-2 present the results and validation respectively of the system response. Validation tests are intended to later test the sensitivity estimates (see Section 3-4) derived from non-causal and causal approaches. This particular type of sensitivity analysis is being used in medicine [24]. Sensitivity helps identify potential risks in the power system.

3. Results

Related tests were performed on the Baba generation, including the AVR and PSS schemes shown in Figure 14. A gain follows the PSS output ('gain2' block in Figure 14) and also tracks frequency changes at the PSS input ('add1' block in Figure 14), both to understand the effect on the system response.

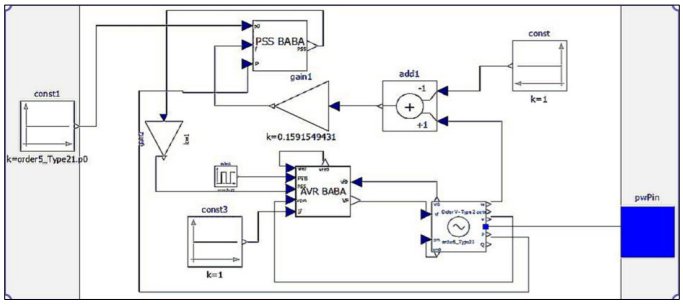


Figure 14: Baba Generator test schema

3.1 Isolated test results

An isolated test of the controller was performed using a 10 second pulse train with amplitude -0.03 starting at 5.65 seconds, so the system returns to normal in 15.65 seconds. The field voltage response under these conditions is shown in Figure 15. In this figure, 'gain2' is set to zero to show only-AVR isolated field and terminal voltages responses.

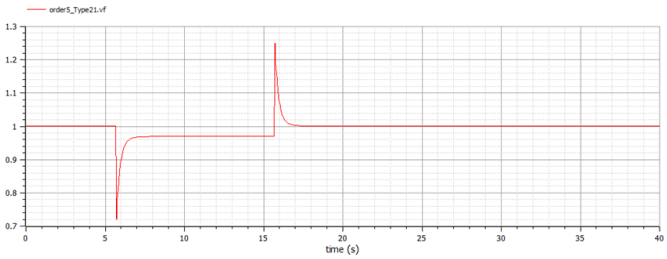


Figure 15: Baba isolated AVR field voltage response - non-causal mode

Figure 15 shows a stable response with a final value of 0.97 pu. Figure 16 shows the non-causal (red curve) and causal (blue curve) electric field voltage responses. Figure 16 shows that both curves are similar. A more detailed analysis of the differences using the mean squared error method follows in Section 3.4.

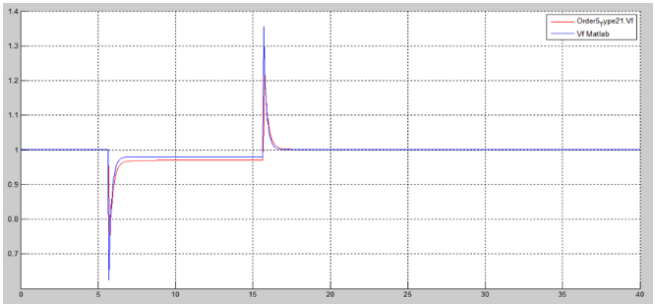


Figure 16: Isolated AVR field voltage response non-causal - causal comparative

Figure 17 shows the terminal voltage (non-causal mode) with the same disturbance as it has a stable response with the electric field voltage. Figure 18 shows a comparison of the terminal voltage responses in the non-causal mode (red curve) and the causal model (blue curve).

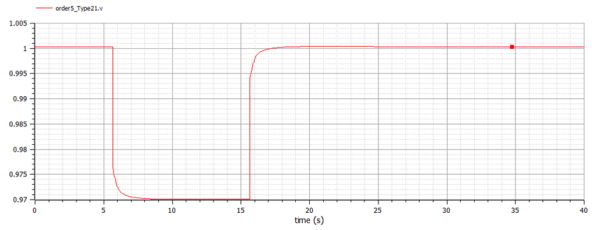


Figure 17: Isolated AVR terminal voltage response - non-causal mode

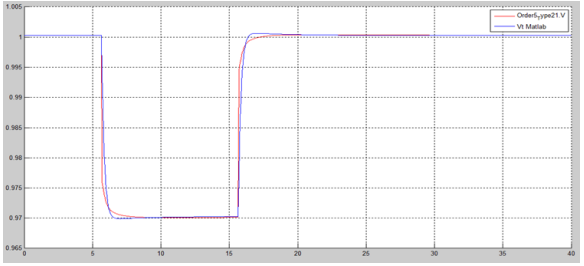


Figure 18: Isolated terminal voltage response non-causal - causal comparative

By changing 'gain2' from zero to one, Figure 19 shows the isolated AVR + PSS field voltage response. Figure 19 shows stable response. Figure 20 shows a comparison of the electric field voltage responses of the non-causal (red curve) and causal models (blue curve) of AVR + PSS. These differences are not relevant.

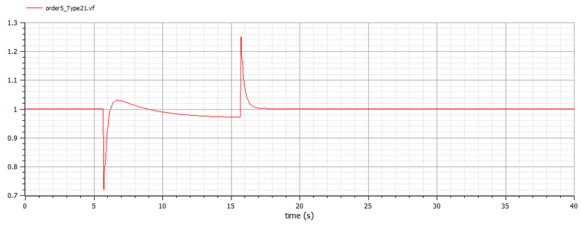


Figure 19: Isolated AVR + PSS field voltage response -- non-causal model

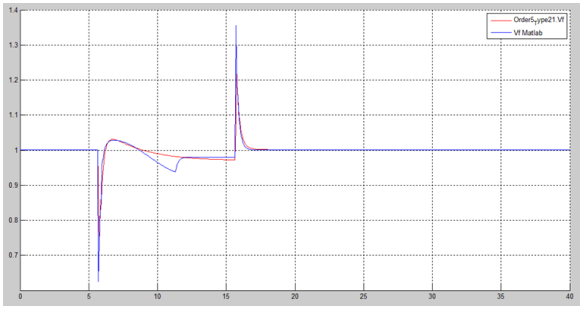


Figure 20: Isolated AVR + PSS field voltage response acasual - causal comparative

The AVR + PSS voltage response is shown in Figure 21 and the comparison is shown in Figure 22. Similar to the field voltage response, there is a stable response and small voltage difference between non-causal and causal modes.

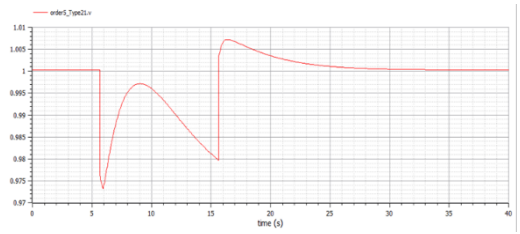


Figure 21: Isolated AVR + PSS terminal voltage response -- non-causal mode

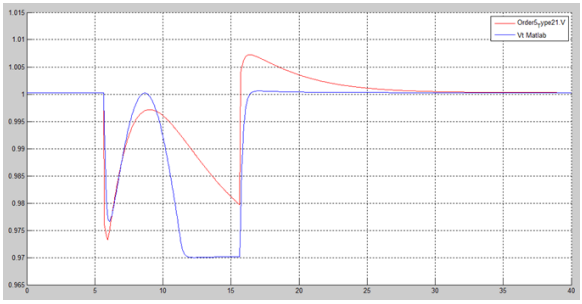


Figure 22: Isolated AVR + PSS terminal voltage response non-causal - causal comparative

In summary, this Section demonstrates the effectiveness of AVR-only and AVR + PSS controllers. This result demonstrates the effectiveness of a fast-response, high gain AVR controller in reducing the power system oscillation stability, thereby improving its transient stability. On the other hand, the AVR + PSS controller reduces transient stability by overriding the voltage signal to the exciter to improve oscillation stability. Basically, the AVR and PSS controller actions are dynamically linked as expected.

In conclusion, both non-causal and causal modes are equally suitable. This reflects the fact that either approach can be used to create schematics of large power grids, once the hard work of creating a model suitable for simulation is completed. Random changes in model parameters are straightforward in the physical (non-causal) declarative equation-based mode.

3.2 NTG results

This Section shows the NTG field voltages and terminal voltages using the infinitive bus described in Section 2.7. An equivalent schema is shown in Figure 13. The same disturbances are used as for the isolated test, i.e., start at 5.65 seconds with and amplitude equal to -0.03 using a pulse train of one period. Figure 23 shows the NTG field voltage in the non-causal model using the AVR controller and Figure 24 shows the AVR field voltage comparing the non-causal and causal responses. Figures 23 and 24 show a stable response.

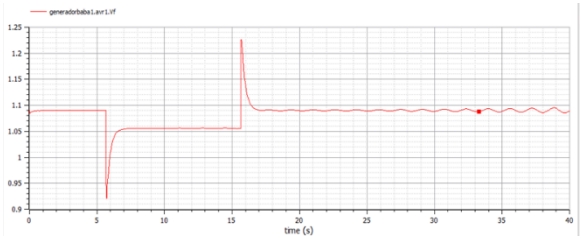


Figure 23: NTG AVR Field voltage response -- non-causal mode

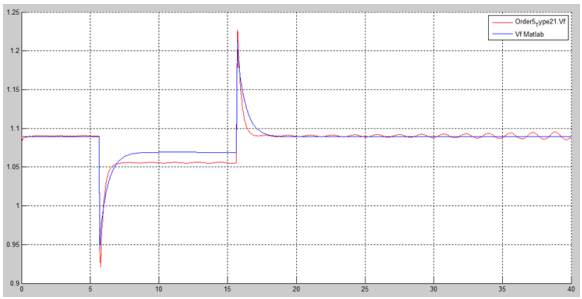


Figure 24: NTG AVR Field voltage comparative non-causal - causal responses

Figure 25 shows the terminal voltage response of the NTG AVR in non-causal mode and Figure 26 shows the NTG AVR response comparing non-causal and causal modes. Figures 25 and 26 show a stable response.

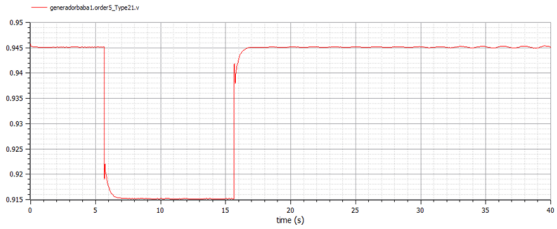


Figure 25: NTG AVR terminal voltage response - non-causal mode

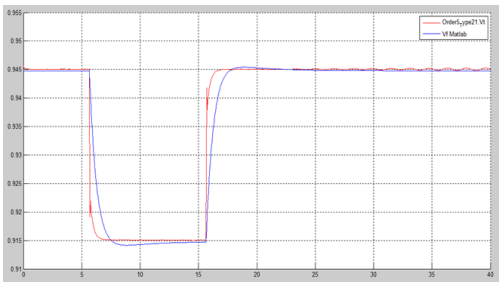


Figure 26: NTG AVR terminal voltage comparative non-causal - causal mode

Figure 27 shows the NTG AVR + PSS field voltage response. Figure 28 shows the comparative non-causal - causal of the NTG field voltage. Figures 27 and 28 show a stable response.

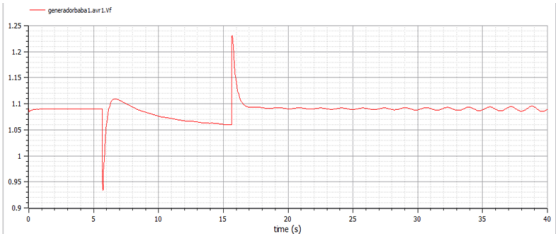


Figure 27: NTG AVR + PSS field voltage response - non-causal mode

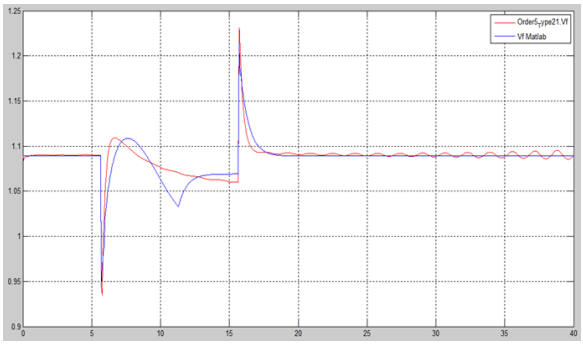


Figure 28: NTG AVR + PSS field voltage comparative non-causal - causal mode

Finally, Figure 29 shows the terminal voltages of NTG AVR + PSS in a non-causal mode, and Figure 30 shows a comparison of terminal voltages in non-causal and causal modes. From Figures 29 and Figure 30 show a stable response.

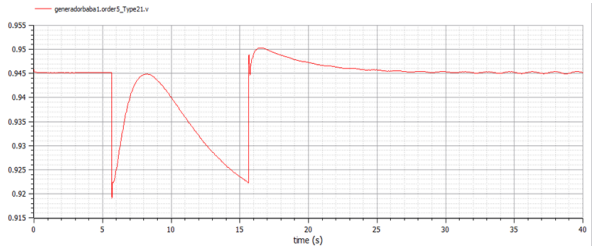


Figure 29: NTG AVR + PSS terminal voltage response -- non-causal mode

The execution time is proportional to its complexity i.e., NTS case study simulation time is longer as expected for the same computer power (see Table 8).

Table 8: Simulation time

Isolated case study: 50.13 s	NTG case study: 1 min 12.63 s

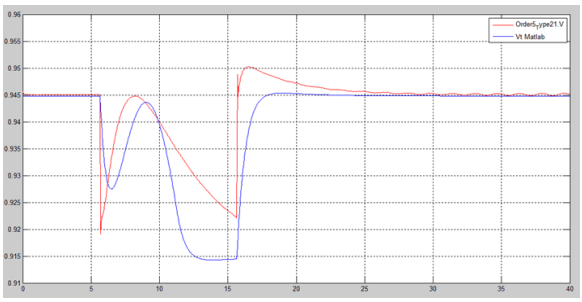


Figure 30: NTE AVR + PSS terminal voltage comparative non-causal and causal modes

In summary, in the Ecuadorian NTG has many disturbances that affect the power grid and can affect the generator reliability. Some disturbances are from large loads. When a large load is suddenly connected to the power grid, the power demand increases as shown in the diagrams of this Section. When a load is suddenly added, the Baba generator frequency begins to oscillate. In the case of small load, oscillation can be damped quickly. Figures of this Section also show that the PSS helps damp these oscillations by modulating the generator excitation.

For a full NTS grid, the grid becomes a complex non-linear system, and is often subject to low frequency oscillations, so these sections were tested with a reduced and simplified scheme [25]. A protective relay system disconnects the generator from the rest of the system and can cause an interruption in the power system.

3.3 Reconciling Non-causal and causal mode

Causal models are based on input-output relationships, while non-causal models describe the power system through implicit differential algebra equations (DAE). A fundamental limitation of the causal approach is the underlying explicit state-space formalism. Causal modelling tools reflects the computational process rather than the structure of the underlying model.

Non-causal model decide how computational causality is automatically assigned by equations rather than causation. While this approach is flexible for the model designer, it does not guarantee a smooth transition from design to simulation results. This is because when assembling multiple models in equations, there are multiple ways to decompose constraints into elementary equations. One of the most common decomposition methods is tearing which determines the computational time required to solve a given system of equations using sparsity patterns [26]. A typical implementation is triangular decomposition of the bottom block where only tearing is applied, which can lead to suboptimal results. A special case of the Dulmage-Mendelsohn decomposition [27] is the Block Lower Triangular (BLT) decomposition. In practice, a common approach to tearing is to perform a BLT decomposition first and then applies tearing to the diagonal irreducible blocks. There are also tearing

heuristics that require BLT decomposition, such as Cellier's tearing [28].

One way to reconcile both models is the root mean squared (RMS) error. The RMS (also known as the quadratic mean) is a special case of the generalized mean with exponent equal to two. RMS is defined as the integral of the squares of the instantaneous difference values during a simulation cycle of two continuously varying functions [29]. Table 9 shows the RMS error for the isolated (left) and NTG (right) case studies. Both cases, only-AVR and AVR + PSS controllers with field and terminal voltage output variables.

Table 9: RMS Isolated and NTG case studies

	Only AVR	AVR + PSS	Only AVR	AVR + PSS
Vf	4.97E-04	5.43E-04	2.09E-04	2.54E-04
Vt	6.19E-06	4.44E-05	1.24E-05	3.79E-05

Table 9 show that the RMS error of the values obtained using the non-causal mode as compared to causal mode over the entire simulation time is almost negligible, so it would be safe to conclude that the outputs are similar.

3.4 Sensitivity Analysis

Sensitivity Analysis (SA) technique consists of varying the input and examining the resulting variation across the output. Saltelli and Annoni [30] argue that local sensitivity analysis examines changes in a models' output variables based on small changes in the model's input parameters. The most common SA practice is One-Factor-at-a-Time (OAT). This consists of analysing the effect of varying one model input factor at a time while keeping everything else constant. In simple terms, sensitivity analysis considers the effect of independent varying parameters. SA is particularly important in this research because the accuracy of power system stability analysis depends on the regulation of the controllers used. Therefore, it is important to attempt to analyse the input controller factors; thus, allowing the planner to better understand of the stability margin of the system. Our sensitivity analysis finds the effect of K_d and T_d in the terminal and field voltages.

The sensitivity analysis case study is related to the NTG case study with an AVR controller with initial values of T_d=5, K_d (derivative gain) = 0, but considering the limits allowed in [31], i.e., for the K_d values between -40 and 0 (typical value of 0) and for T_d (smoothed time constant) values between 0.1 s and 10 s (typical value of 5 s). Table 10 shows variations in percentage for field voltage and terminal voltage for K_d values of -5, -15 and -30 and T_d values of 1 and 10.

Table 10 shows that K_d is a very sensitive parameter. When the ARV K_d value is at the upper limit, the terminal voltage fluctuates by 6.693 percent. Therefore, a fast response AVR impacts both the oscillation stability as well as increasing transient stability of the power system.

Table 10. NTG AVR OAT Sensitivity Analysis

	Terminal Voltage (RMS percent variation)	**Field Voltage (RMS percent variation)**
K_d = -5	0.425	1.728
K_d = -15	1.491	5.512
K_d = -30	3.390	6.693
K_d = -1, T_d = 10 s	0.692	2.878
K_d = -1, T_d = 1 s	1.023	2.7020

4. Discussion

Section 2 shows how to estimate the Baba-generated field and terminal voltages in AVR and AVR + PSS controller modes using two case studies, i.e., isolated and NTG connected. Section 3 presents the application of this methodology to estimate the field voltage and terminal voltages in Baba generation. Case studies differ in system complexity. Section 3 is also an extension to the traditional sensitivity analysis, deconstructing the inputs to the path as the AVR derivative parameters flow through the Baba system and performing an innovative `what-if parameter sensitivity' scenario analysis. In this section, the methods, chart/table results, and sensitivities used to estimate the Baba generation are described in a broader context and discussed.

This paper began with a description of the power generation unit, AVR and PSS controller models, Transformers, Transmission lines and Infinite buses forming a simplified learning system (see Section 1). Two controller approaches: Only--AVR and AVR + PSS were developed in this research. In particular, the only-AVR controls the gate opening of the thyristor of the controlled rectifier. The entire system that controls and generates the excitation voltage is called the excitation system. For AVR + PSS controller, the main reason for implementing a PSS in the voltage regulator is to improve the small signal stability characteristics of the system. This study has shown that there is a trade-off between synchronous torque provided by the AVR and damping torque provided by the PSS.

This research has shown first and foremost that Generation data set components (see Section 2.1) are generally available in some form to many, if not all, Generation Business Units. Non-causal and causal models coexist as collaborative tools for simulating variables of interest in the simulation. The RMS error analysis using the non-causal mode is almost negligible compared to causal mode over the entire simulation time, so the outputs can be considered similar (see Section 3.3).

One of the issues highlighted is that in the initial phase of this research involved substantial data management,

cleansing, restructuring and additions to the NTG initial data set in PF package and the spatial extent complexity of the NTG case study surrounding Baba system. This study supports energy companies and stakeholders to model control systems in several ways: the first using either causal models based on input-output relations or non-causal models using implicit Differential Algebraic Equation (DAE). Second is the methodology for building the power generation control system. Third, to assess the impact of interventions, we explore the available tools that policy makers and city energy planners may need to identify reliability issues in the national power system.

In summary, this study has integrated a number of data sets in a way that it was able to integrate with well-respected standards such as the IEEE 421.5 standard, so every individual generation business unit can replicate this work. There are also issues with data collection methods and distribution restrictions.

This research proved that the strength is the framework approach not necessarily the model. The non-causal chosen is not necessarily suitable for large power systems. Therefore, an interesting application for future work is to take the framework developed in this study and adapt it to another hybrid model. This hybrid model can integrate power flow to control the physical properties of the system and multiple generators and their interrelations.

4. Conclusions

This study has shown that generation units' controller is affected by its parameters in all case studies. In some cases, these properties lead to output responses, suggesting that care should be taken when designing controller parameters from other studies instead of rigorous local analysis.

This paper proposes AVR and PSS with output limiters. This is because the key parameters that need to be controlled and kept within reasonable limits are the over-excitation and under-excitation indicators on the AVR output and saturation on the PSS output.

The stability analysis did not include models for low voltage load characteristics, tap changer behaviour under load, and relay protection, so the analysis includes manual manipulation. Further refinement of the stability analysis should include a physical understanding of these factors.

The work carried out within the framework of this research will make an important contribution to the research field of energy system modelling in several respects. First, the methodology used will greatly expand our theoretical understanding of existing complexities; second, to find new useful platforms to study power systems with their respective controls, with real conditions facilitating the study of different scenarios; and finally get the support of different tests and arrive at the same set of answers.

References

[1]. International Renewable Energy Agency, "Sustainable development goal 7: Energy indicators". Technical Report. IRENA, 2017. URL: https://www.irena.org/IRENADocuments/Statistical_Profiles/SouthAmerica/Ecuador_SouthAmerica_RE_SP.pdf.

[2]. Food and Agriculture Organization of the United Nations, "Ecuador General Information". *Technical Report. FAO*, 2021. URL: http://www.fao.org/3/Y4347E/y4347e0n.htm.

[3]. J.P. Hidalgo-Bastidas, R. Boelens, "Hydraulic order and the politics of the governed: The Baba dam in coastal Ecuador". *Water* 11, 2019. URL: https://www.mdpi.com/2073-4441/11/3/409.

[4]. M. Ilic, J. Zaborszky, *Dynamics and Control of Large Electric Power Systems*. Wiley-IEEE Press, 2000.

[5]. IEEE Power Engineering Society, *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies*. Technical Report, 2006.

[6]. NERC, *Steady-State and Dynamic System Model Validation*. Technical Report, 2017.

[7]. A. Elices, L. Rouco, H. Bourles, T. Margotin, "Design of robust controllers for damping interarea oscillations: application to the European power system". *IEEE Transactions on Power Systems* 19, 1058-1067, 2004. doi:10.1109/TPWRS.2003.821612.

[8]. P. Verdugo, J. Játiva, "Metodología de sintonización de parámetros del Estabilizador del Sistema de Potencia -PSS" [Power System Stabilizer parameter tuning methodology -PSS]. *Revista Técnica Energía* 10, 2014.

[9]. NASPI, *Model Validation Using Phasor Measurement Unit Data.* Technical Report, 2015.

[10]. W. Vargas, P. Verdugo, "Validación e identicación de modelos de centrales de generación empleando registros de perturbaciones de unidades de medición fasorial, aplicación práctica Central Paute – Molino" [validation and identication of generation plants models using disturbance records from phasor measurement units, practical application Paute - Molino Power Plant]. *Revista Técnica Energía* 16., 2020.

[11]. A. Bartolini, F. Casella, A. Guironnet, et al., "Towards pan-european power grid modelling in Modelica: Design principles and a prototype for a reference power system library", *13th International Modelica Conference*, pp. 627-636, 2019.

[12]. F. P. Demello, C. Concordia, "Concepts of synchronous machine stability as affected by excitation control". *IEEE Transactions on Power Apparatus and Systems PAS*-88, 316-329, 1969. doi:10.1109/TPAS.1969.292452.

[13]. P. Kundur, N.J. Balu, M.G. Lauby, *Power system stability and control*. New York: McGraw-Hill, 1994.

[14]. P. Fritzson, *Introduction to Modeling and Simulation of Technical and Physical Systems with Modelica*. Wiley-IEEE Press, 2011.

[15]. Consorcio Hidronergético del Litoral, *EIA definitivo Proyecto Hidroeléctrico Baba* [EAI final Baba Hydroelectric project]. Technical Report, 2006

[16]. L. Qi, "Modelica Driven Power System Modeling, Simulation and Validation". (Master's thesis, Royal Institute of Technology, 2014).

[17]. T. Van-Cutsem, L. Papangelis, *Description, Modeling and Simulation Results of a Test System for Voltage Stability Analysis*. Technical Report, 2013.

[18]. M. Baudette, M. Castro, T. Rabuzin, J. Lavenius, T. Bogodorova, L. Vanfretti, "Openipsl: Open-instance power system library | update 1.5 to itesla power systems library (ipsl): A modelica library

for phasor time-domain simulations". *SoftwareX* 7, 34-36, 2018. URL: https://www.sciencedirect.com/science/article/pii/S2352711018300050, doi :https://doi.org/10.1016/j.softx.2018. 01.002.

[19]. D. Mota, *Models for Power System Stability Studies, Thyricon(R) Excitation System*. Technical Report, 2010.

[20]. K. Walve, "Modelling of power system components at severe disturbances", *International conference on large high voltage electric systems*, 1986.URL: https://e-cigre.org/publication/38-18_1986-modelling-of-power-system-components-at-severe-disturbances.

[21]. IEEE Power and Energy Society, *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies (Revision of IEEE Std 421.5-2005)*. Technical Report, 2016.

[22]. K.E. Bollinger, S.Z. Ao, "PSS performance as affected by its output limiter". *IEEE Transactions on Energy Conversion* 11, 118-124, 1996. doi:10.1109/60.486585.

[23]. P.M. Anderson, A.A. Fouad, *Power System Control and Stability*, Wiley-IEEE Press; 2nd edition, 2002.

[24]. V. Bari, E. Vaini, V. Pistuddi, A. Fantinato, B. Cairo, B. De-Maria, L.A. Dalla-Vecchia, M. Ranucci, A. Porta, "Comparison of causal and non-causal strategies for the assessment of baroreflex sensitivity in predicting acute kidney dysfunction after coronary artery bypass grafting". *Frontiers in Physiology* 10, 2019.

[25]. E.V. Larsen, D.A. Swann, "Applying Power System Stabilizers part iii: Practical Considerations". *IEEE Transactions on Power Apparatus and Systems PAS*100, 3034-3046, 1981. doi:10.1109/TPAS.1981.316411.

[26]. A. Baharev, A. Neumaier, H. Schichl, "Failure modes of tearing and a novel robust approach", *Proceedings of the 12th International Modelica Conference* pp 15-17, 2017.

[27]. A. Pothen, C.J. Fan, "Computing the block triangular form of a sparse matrix". *ACM Transactions on Mathematical Software*. 16, 303-324, 1990. URL: https://doi.org/10.1145/98267.98287, doi:10.1145/98267.98287.

[28]. P. Tauber, L. Ochel, W. Braun, B. Bachmann, "Practical realization and adaptation of Cellier's Tearing Method", *Proceedings of the 6th International Workshop on Equation-Based Object-Oriented Modeling Languages and Tools, Association for Computing Machinery*, New York, NY, USA. p. 11-19, 2014. URL: https://doi.org/10.1145/2666202.2666204,doi:10.1145/2666202.2666204.

[29]. M.J. Gibbard, P. Pourbeik, D.J. Bowles, "Small system stability, performance and control of power systems". *University of Adelaide Press*, 2015. Adelaide.

[30]. A. Saltelli, P. Annoni, "How to avoid a perfunctory sensitivity analysis". *Environmental Modelling and Software* 25, 1508-1517, 2010. URL: https://www.sciencedirect.com/science/article/pii/S1364815210001180, doi: https://doi.org/10.1016/j.envsoft.2010.04.012.

[31]. A. Hammer, "Analysis of IEEE Power System Stabilizer Models". (Master's Thesis. Norwegian University of Science and Technology, 2011). URL: https://ntnuopen.ntnu.no/ntnu-mlui/bitstream/handle/11250/257120/445805_FULLTEXT01.pdf?sequence=1.

JAVIER URQUIZO, after an undergraduate degree in Electric Power Systems in Ecuador, I did graduate master school in United States having a master's in electrical engineering from Stevens Institute of Technology, Hoboken New Jersey and a master's in civil and Environmental Engineering from University of New Orleans, Louisiana. I went to the United Kingdom in 2011 to pursue a doctoral degree in the Planning of Urban Energy Systems at Newcastle University. I did my VIVA in June 2015. The monograph I submitted informs domestic energy demand estimates to a number of EU, UK and Local Authority carbon and energy efficiency schemes. Currently I am doing research and teaching in an Ecuadorian University ESPOL, currently teaching Electric Power Distribution Systems, Renewable Processes and Sustainable Energy System Planning.

DIOVER BONILLA, after an undergraduate degree in Electric Power Systems at Escuela Superior Politécnica del Litoral ESPOL - Ecuador, I did graduate school in Renewable Energy I the European Centre of postgraduate studies, Madrid - Spain.

FRANCISCO RIVERA, I have an undergraduate degree in Electric Power Systems at Escuela Superior Politécnica del Litoral ESPOL – Ecuador

ROMMEL CHANG After an undergraduate degree in Electric Electronics and Industrial Automation at Escuela Superior Politécnica del Litoral (ESPOL), I did graduate school in Industrial Automation and Control at ESPOL. I work at Baba Generation Plant.

Received: 31 October 2022, Revised: 22 December 2022, Accepted: 29 December 2022, Online: 28 January 2023
DOI: https://dx.doi.org/10.55708/js0201002

CAPEF: Context-Aware Policy Enforcement Framework for Android Applications

Saad Inshi [1], **Mahdi Elarbi** [1], **Rasel Chowdhury** [1,*], **Hakima Ould-Slimane** [2], **Chamseddine Talhi** [1]

[1] Department of Software Engineering and Information Technology, École de technologie supérieure, Montréal, Canada
[2] Département de Mathématiques et d'Informatique, Université du Québec à Trois-Rivières, Trois-Rivières, Canada
*Corresponding author: rasel.chowdhury.1@ens.etsmtl.ca

ABSTRACT: The notion of Context-Awareness of mobile applications is drawing more attention, where many applications need to adapt to physical environments of users and devices, such as location, time, connectivity, resources, etc. While these adaptive features can facilitate better communication and help users to access their information anywhere at any time, this however bring risks caused by the potential loss, misuse, or leak of users' confidential information. Therefore, a flexible policy-based access control system is needed to monitor critical functions executed by Android applications, especially, those requiring access to user's sensitive and crucial information. This paper introduces CAPEF, which is a policy specification framework that enforces context-aware inter-app security policies to mitigate privacy leakage across different Android applications. It also, provides an instrumentation framework to effectively enforce different behaviors based on automated context-aware policies to each Android application individually without modifying the underlying platform. Accordingly, the modified applications will be forced to communicate with our centralized policy engine to avoid any malware collusion that occur without the users' awareness. Experiments conducted on CAPEF shows an effective performance on the size of the enforced application after the instrumentation. The average size added was 705 bytes, which is about 0.063% of the size of the original applications, which is significantly small compared to other existing enforcement approaches. Also, we have denoted that the size and the execution time of the policy increases whenever the policies become more complex.

KEYWORDS Security, Android applications, Application instrumentation, Context-aware policies, Policy enforcement, Privacy

1. Introduction

Context awarenes service is a key driver for the modern mobile operating systems which are commonly prompting users by showing authorization dialog boxes asking for allowing or denying access to some functionalities. These services opened a big interest in defining, managing, and enforcing context-aware policies especially for those scenarios that put users under the risk of leaking or misusing their credential information. Yet, thousands of malicious applications are developed on the Android store and affecting millions of Android users worldwide. To safeguarded Android users, Google is frequently announcing the cracking down of such malicious applications. For instance, Google has removed over 700,000 malicious applications from the Play Store in 2017 only [1]. Based on Goggle statistics, this is 70% more than what Google removed in 2016. Very recently in 2022, Google has removed 16 bad apps that missuses mobile data and draining batteries. Surprisingly, these apps have been downloaded by more than 20 million users around the world [2].

Android system protects sensitive APIs by granting them permissions to amplify application privileges on the device, including access to stored data and services, such as network, memory, and so on. All permissions required to access the protected APIs in each application's manifest file (AndroidManifest.xml) [3] are necessarily set by the Android app developers. System permissions are divided into two categories, normal and dangerous. Normal permissions do not pose a direct threat to the privacy of the user, although dangerous permissions may allow the application to access the user's confidential data. Existing application authorization system in Android allows you to control only the permissions that are classified as dangerous, whereas our developed policy approach, offers the ability to control all monitored permissions as any application may cause a risk or conflict within a specific context without user awareness. Also, our model will mitigate malware collusion in which two or more malicious apps combine to accomplish their goals. For example, a user can choose to allow a camera app to access the camera, but not to the contact information without his consent or awareness. Another example, where normal applications can be granted permissions to collecting user's contacts, photos, videos,

locations, or banking information then sending it over the internet to a remote server and taking into consideration pre-defined context aware access control policies. Therefore, a flexible policy-based access control system is needed to monitor APIs functions in Android applications, especially those requiring access to the user's sensitive and crucial information. The current permission system of Android still has some limitations, where users must grant most permissions requested by an application to install it, without being able to automatically manage most of these permissions based on the user's context afterwards.

This drawback has motivated the researchers to propose context-aware policies and/or define policy languages to enforce the current Android permission system either by modifying the Android platform such as in [4]–[8] or by instrumenting the Android Applications [9]–[18] and more recently in [19]–[21] (more details and comparisons can be seen in the background and literature review section). While, existing works have demonstrated significant effectiveness in protecting users against threats, these approaches are still impeded by several drawbacks.

1.1. Challenges

Defining and monitoring context-aware inter-app policies of sensitive APIs on Android applications presents several challenges. Especially, when we are trying to defend applications collaborating to create malicious contexts:

i Context-aware inter-app policies are difficult to predict as they frequently get changed and need to be updated accordingly for accuracy and correctness.

ii Beside the difficulty of representing the security policies in a logical language which can contain user contexts and semantics, a key challenge is how to design and develop effective and efficient algorithms to monitor private information leakage on semantics levels.

iii There is a need for a policy language that can provide certain agreements that empower users with the ability to prioritize specific mobile resource and specify the amount and kind of information that can be shared within particular contexts. For instance, a user should be able to share a personal data with a specific service provider based on his location or at a specific time of the day to ensure his privacy. In this case, the user must agree on a trade-off between data privacy and the needed service. As a result, a policy should be defined to ensure privacy, while certain context-based information can be shared.

iv Android Sandboxing is introduced in the recent Android version 13.0. Sandboxing protects apps data and permission from getting access from other apps. This new feature will have an impact on our inter-apps policy model, but our main goal still effective which is to allow the user to define his policies to work automatically depending on the context update, to the running apps etc. Therefore our, framework can fully protect the Android OS versions lower than 13.0 in which the installed apps can communicate between each others.

v Due to the resourced constrained mobile devices, we have to decide, in early stages the instrumentation and monitoring location, whether to be on device, external PC or App market.

1.2. Contributions

This article is contributing solutions for the above-mentioned challenges and limitations by introducing:

i A formal context-aware policy specification framework for Android applications that effectively describe users defined consents.

ii A design and implementation of an instrumentation framework to mitigate privacy leakage across different Android applications.

iii Providing a centralized applications controller. This will allow users to manage all API calls performed by the applications installed on the device and to mitigate malware activities.

iv Effectively enforce different behaviors based on automated context-aware policies for each Android application individually without any modification to be entailed in the underlying platform.

v Experiments conducted on our CAPEF in terms of performance by analyzing the size of the enforced application after the instrumentation, also, the execution time of the policy decision, and the policy size which affects the complexity of the applied rules and conditions.

2. Background and Literature review

Android applications are distributed as APK files (Android Package). Each package consists of the application's manifest file, resources and application bytecode encoded for the Dalvik Virtual Machine (DVM) as a single classes.dex file. The APK file has to be signed for verifying its authenticity. Android signed package (Dex files) runs separately in its own DVM. Also, Android system is an open source platform where applications are published in different markets without being monitored or analyzed to guarantee their behavior. For that reason, Android platform protection mechanisms such as Application Sandboxing, Permission Model and Application Signing are developed for privacy and security purposes. Accordingly, at the time of installing Android applications, each application will get a unique user identifier (UID) [22]. Also, no application will be able to access other application's files. Besides, every application run into separate VMs. Accordingly, no vulnerable application will affect other applications.

For Android access control policies, context awareness have become an essential accessory in most mobile platforms and applications. This necessity has motivated many researchers to provide policy enforcement mechanisms to

define, manage and enforce different context aware policies. In this context, traditional access control models which generally refer to the process of determining what actions are allowed by a given subject upon objects and resources should be reinforced to fulfill the modern context-aware applications.

The most popular access control models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) [23] . For instance, RBAC is a model that uses "roles" to determine access control, also permissions are associated with these roles, and users are made members of appropriate roles. In ABAC, requests are granted or denied based on subject and resource attributes, environment conditions, and a set of policies specified in terms of those attributes and conditions. When it comes to using ABAC models, one of the well-known standard system implementations is XACML [24]. The XACML standard defines a declarative access control policy language implemented in XML and provides a processing model on how to evaluate access requests.

Thus, to adopt an effective context-aware access control model on Android platform and its application, there are series of work studying and proposing security mechanisms for privacy and security requirements. In this context, many reviewed efforts in [4]–[8] have been developed to extend the Android security framework in order to improve the standard permission control provided by the operating system. For example, SecureDroid [4] addressed the issue of controlling security policies while applications are executing in the Android environment. During the installation of an application, Android allows the user to grant permission for an application to use certain features of the system. Therefore, SecureDroid introduced an extension of Android's security framework in order to improve the standard permission control provided by the operating system. To achieve this goal, they introduced a new control mechanism adding granularity and flexibility. Moreover, their policy framework is based on customizing the XACML standard to work on the Android system. Also, they have provided the ability to add or edit a policy through a dedicated system service. This will allow users to specify which permissions to grant and which others to deny for each of the defined contexts.

However, modified Android platform has a number of major drawbacks such as the need of building different versions of firmware and platform codes, where applications will be limited by the security policies supported by the modified Android platform. Therefore, many researchers in [9]–[18] and more recently in [19]–[21] have provided solutions that are based on instrumenting Android Applications in ordered to enforce some security policies. These solutions require no modification to the Android platform and can be easily deployed. For instance, Aurasium [9] is a concurrent approach that rewrites Android application to sandbox important native API methods and monitors the behavior of the application to detect any security violations. Also, Capper [17] is a prototype for context-aware policy enforcement to mitigate privacy leakage in Android applications. This mechanism will enforce privacy policy based on user preferences. By using this system, when a user tries to install any Android application the bytecode rewriting engine called BRIFT will rewrite the program of this application by selectively inserts instrumentation code along taint propagation slices for monitoring and preventing any information leakage. Another interesting research called Weave Droid [18] has provided a framework for weaving AspectJ aspects into an Android application. The framework takes two inputs at the beginning: APK and a set of aspects that will be weaved into the APK. The weaving process will be performed on the Android device. Also, very recently in [21] They have developed a lightweight monitoring system to detect malware activities with the log file and they evaluated the proposed model according to Policy-based permissions.

Accordingly, some of the reviewed frameworks have provided enforcement mechanisms to mitigate Malware activities by enforcing context-related policies, however they didn't afford a policy specification language that runs on Android system as an application or a service without modifying the Android platform. Thus, this article is introducing a more featured policy specification language that allow regular users and any company to easily interpret and enforce their complex context-aware inter-apps policies on their Android mobile applications.

2.1. Summary of the literature reviews

The table 1 shows the summary and differences between our research and the other works.

3. System Overview

This section gives an overview of our approach that automatically enforces user specific context-aware policies for android application and monitors all API calls that occur due to the interaction between enforced applications. Our developed system works in the application level of the Android framework, and its main components are illustrated in Fig. 1.

i From left, the first components represented the instrumentation of the targeted Android application (byte code or source code) by injecting monitoring code before each selected API method's call to intercept it at run time.

ii After the instrumentation, the applications will be forced to communicate with our controller that monitors the targeted context-aware inter-app calls.

iii Then, users will use CAPEF interface to create context-based rules and conditions in the form of security and privacy policies. More precisely, the policy represents a rule or set of rules based on a set of conditions and save it in the policies Database.

To motivate and illustrate our approach, we present the following scenario for vulnerability pattern that consider context-awareness policies. In this scenario, a user is using a public WiFi network in a coffee shop and he is trying to consult his credential banking information through his banking application. As the public network is not secure

Table 1: Comparison of related work

Approach/ System	Methodology	Required modification	Policy Language	Context-aware inter-app Privacy Leakage Prevention
TaintDroid [25]	Dynamic Analysis	Android Platform	✗	✗
Appink [26]	Watermarking	Application	✗	✗
Apex [5]	Policy Enforcement	Application	✗	✗
TISSA [6]	Resources Access Control	Android Platform	✗	✗
AppFince [7]	Dynamic Analysis & Resources Access Control	Android Platform	✗	✗
Aurasium [9]	Rewriting Java Bytecode	Application	✗	✗
I-arm-droid [11]	Rewriting Dalvik bytecode	Application	✗	✗
AFrame [14]	Isolating Advertisements	Application	✗	✗
Capper [17]	Rewriting Java Bytecode	Application	✗	✗
SecureDroid [4]	Policy Enforcement	Android Platform	✓	✗
Weave Droid [18]	Isolating Advertisements	Application	✗	✗
[21]	Policy-based permissions	Application	✗	✗
CAPEF	Policy Language	Application	✓	✓

and there are other people who use the same network, so there is a risk of sending requests to attackers and thefts of private data. Android system checks only if the user has been previously granted the permission of accessing WiFi network and doesn't provide any context-awareness policies to mitigate such dangers scenarios. CAPEF can provide more effective access control not only on the permissions declared in advance by the user but also at run time based on the context of the user, device, and resources. Thus, as a solution to the above-mentioned scenario, a user can use CAPEF to define a policy that prevent the use of banking applications while connecting to a public WiFi network. When an enforced bank application attempt to get public WiFi access, our application controller will first check if the permission is declared in the application manifest file. Then, will check if the user has defined any policies related to this permission in the policies database. Subsequently, the controller access decision will be based on the predefined policies for that specific API. As a result, the controller will notify the user for not being allowed to connect to public WiFi for banking activities.

4. CAPEF

Context-Aware policies are not static and might be changing over time to fulfill users' needs. Therefore, these policies could be used to control the behavior of the applications during run-time, which in our case, means monitoring and controlling all sensitive activities across different applications according to user's context. To achieve this goal, we provided a native Java-based CAPEF that allow regular users and enterprises to interpret and enforce their complex context-Aware policies. Contexts will represent various parameters including time, location, identity, activity, application, device status, resources etc. Moreover, these policies can be exported in multiple formats such as XML and JSON as they are widespread use today for data interchange and structured stores.

To develop the CAPEF language that allows the user to define contextual policies and transform them into security controls, we must rely on a flexible design that varies with the complexity of the policies, rational, able to execute all the conditions and easy to add new contexts.

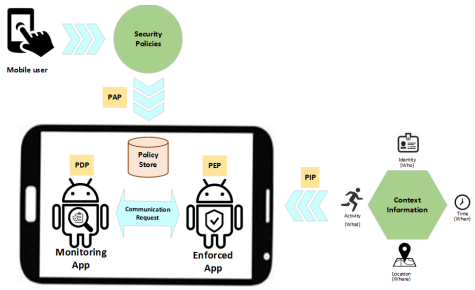


Figure 2: CAPEF Architecture

4.1. CAPEF Architecture

The main components of CAPEF are shown in Fig.2. which represents the following:

i **Security policies**: which is an interface for the user to define context aware policies and save them at the policy store. This component will act as a policy administration point (PAP) which is the source of the policies.

ii **Enforced Application**: Which plays the role of policy enforcement point (PEP) that receives the access request and move it to the Monitoring application for making access decision based on the predefined context aware policies.

iii **Context Information**: Provides context information in a form of attribute values about the targeted applications, resources, activates, actions and so on. This component will play the role of policy information point (PIP) in our system.

iv **Monitoring Application**: This component plays the role of policy decision point (PDP). It takes the access request from the PEP then interacts with PAP and PIP that capture the required context information to identify the appropriate policy. Then evaluates the

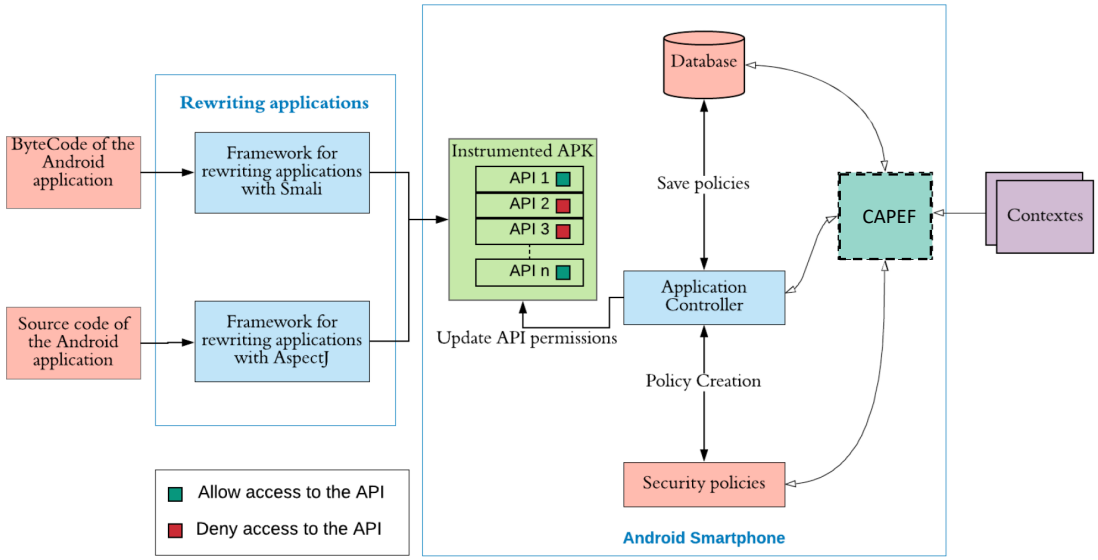


Figure 1: System Overview

request according to the applicable policy and returns the decision to the PEP.

4.2. Formal Definition

Hereafter, we formally define our ABAC policy model, which is composed of three main entities:

1. A, P, and C : sets of application, permissions (resources) and contexts, respectively;
2. AA , PA ,and CA are the pre-defined sets of attributes for applications, permissions, and contexts, respectively.

I An application *app* is a represented by a tuple as follows:

app <name, visibility, class, APIs>, where:

i visibility ∈ {background, foreground}

ii class ∈ { banking, communication, recording, games, media, location}

iii APIs: a set of APIs that can be invoked during execution

II A permissions *per* embeds the access to the resource, it is a represented by a tuple as follows:

per < name, resource, securityLevel >,

i resource ∈ { personal data, calendar, camera, wifi, account, calls, sms,Audio, GPS},

ii securityLevel ∈ { Normal, Dangerous },

III A context *c* is a represented by a tuple as follows:

c < time, location, fgApp, BgApps availableCPU, availableMEM, availableNRG >,

i fgApp indicates which application is running in foreground;

ii BgApps is the set of the applications running in background.

3 Attr(*app*),Attr(*per*), and Attr(*c*) are attribute assignment relations for application app, permission per and context c, we have respectively

I Attr(*app*) ⊆ name × visiblity × class × APIs;

II Attr(*per*) ⊆ name × resource × securityLevel;

III Attr(*c*) ⊆ time × location × fgApp × BGaps × availableCPU × availableMEM × availableNRG.

For the value assignment of each attribute, we use the following notation: **entity.attribute= value** ,

For example, for an application **app**, a permission **per** and a context **c**, we have the following assignments:

app.visiblity = 'background', per.securityLevel = 'Dangerous', c.location = 'Montreal'.

4 The ABAC policy rule that decides whether or not an application **app** is allowed is allowed to get the permission **per** under a particular context **c**, is denoted as a predicate **PR** over the attributes of **app**, **per** and **c** as follows:

Rule : Allow(app, per, c) ← PR(Attr(app), Attr(per), Attr(c))

Given all the attribute assignments of *app*, *per*, and *c*, if the predicate's evaluation is true, then the application **app** is allowed to get the permission **per** under the context **c**; otherwise, the permission is denied. Using the formal definition, we can have different types of policies for the *app*, for example:

1. A rule that dictates that " When a banking applications is being used, so the TakeScreenshot actions should be prevented from running" can be written as:

   $Allow_{screenShot}$(app, per, c) ← (TakeScreenshot ∈ app.APIs) ∧ (per.resource==screen) ∧ (c.fgApp.class != banking)

2. A rule that dictates: "RecordVoice and RecordCall applications should be prevented from running when the user is dialing Skype from 9:00 to 10:00" can be written as:

   i $Allow_{recordVoice}$(app, per, c) ← (RecordVoice ∈ app.APIs) ∧ (per.resource==voice) ∧ ((c.fgApp != 'skype') ∨ (c.time <9:00 am ∨ c.time > 10:00am))

   ii $Allow_{recordCall}$(app, per, c) ←(RecordCall ∈ app.APIs) ∧ (per.resource==call) ∧ ((c.fgApp != 'skype') ∨ (c.time < 9:00am ∨ c.time > 10:00am))

   Or simply by combining the two rules as following:

   $Allow_{record}$(app, per, c) ←(RecordVoice , RecordCall ∩ app.APIs!= ϕ) ∧ (per==voice ∨ per==call) ∧ ((c.fgApp != 'skype') ∨ (c.time < 9:00am ∨ c.time > 10:00am))

4.3. CAPEF Policy Specification

CAPEF language is based on the definition of a policy that consists of a user ID, a policy name, a policy execution state, a control rule, and a list of applications to control. Each of these applications is characterized by a name, package name, execution status and a list of permissions. The permissions consist of a name and a execution state. The security rule consists of a list of objects that can be Parentheses, Conditions, Logical Operators, Conditional Operators, CPU, Time, Resource Used, Location and Battery.

As shown in Fig.3, user-defined security policies and its rules can contain multiple conditions, different contexts, multiple logical operators, and parentheses to specify priority between conditions. Also, these policies can be executed simultaneously in different inter-app activities across different applications. In this case, policy decision becomes more complex. Therefore, to facilitate and accelerate the execution of any compound policy, our algorithm will receive the current contexts and the control rule as parameters then returns the policy decision of the controller.

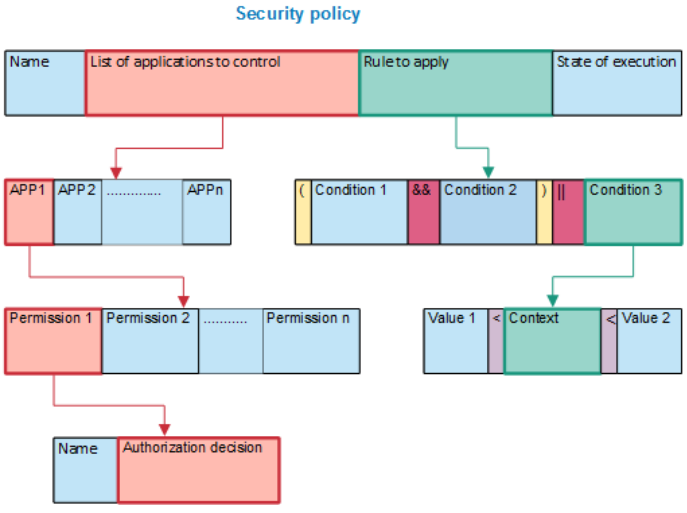


Figure 3: CAPEF Policy Execution Structure

In addition, the security rule might have sub-nodes of other rules, and themselves are sub-rules of the main rule. Therefore, we have adopted a recursive technique to reduce the complexity of the composed security rules. In this case, the algorithm will call itself, and recursion stops condition must be checked, otherwise the program will be stuck in an infinite loop.

To show the usefulness of our solution, we have chosen two examples of dangerous scenarios and we will translate them into security policies.

I Critical scenario 1: If the user uses his banking application to check his data and deposit a check in his account, while a TakeScreenshot application is installed on his smartphone.This application that takes screenshots automatic present a risk on banking data that is personal life data.

   i Solution: You must prevent the TakeScreenshot application and any screenshot function from running when the user is using their banking application.

   ii Security Policy: If [BankApp] is running, then stop the [TakeScreenShot] application.

II Critical Scenario 2: If the user is in a private work meeting every Monday from 9:00 am to 10:00 am by Skype while many other apps are able to record his speech and share it in public as RecordVoice and RecordCall applications.

   i Solution: RecordVoice and RecordCall applications should be prevented from running when the user is dialing Skype from 9:00 to 10:00.

   ii Security Policy: If ((CALL_PHONE in [Skype]) && (9: 00 <= Current_Time <= 10: 00)), then stop or prevent (if not yet executing) the application [RecordVoice && RecordCall].

To apply and evaluate the defined context aware policies, an application controller has been developed to allow users to define policies depending on different types of contexts and conditions.

5. Centralized Application Controller

The developed controller provides a user interface to translate the dangerous scenarios into security policies using the CAPEF. Based on the defined policies, the controller will make the adequate access control decision to allow or block applications from using certain permissions. Moreover, provide centralized control of installed applications which capture mandatory decisions that are automatically dependent on the current context.

Fig. 4, shows an example of how to define a security policy with our controller. The control scenario is to block the execution of the Camera resource in the Camera application if the user is in a meeting from 10:30 to 11:30 or from 13:30 to 15:30 otherwise it is in a meeting from 15:30 to 15:40 and that Bluetooth is enabled in the BluetoothShare Application.

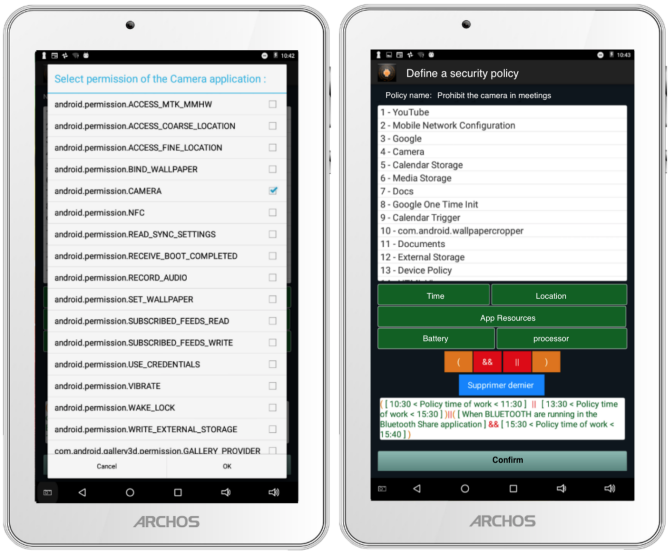


Figure 4: Screenshots of a policy definition within our controller

5.1. Managing Security Policies

The Application controller interface has been developed in a way that the user will be able to define any security policies in a few simple clicks. We chose our solution to be ergonomic, personalized, and user-centric design to have a convenient and easy-to-use service. It has also been taken into consideration that our user interface must reduce the search effort and limit data entry. In addition, all policies created by the user have been saved in a database. With the database, the user will be able to import, create, view, and modify security policies.

5.2. Export/Import Security Policies

Our developed solution allows the user to extract his defined policies and share them with other users of the controller or send them to nay server or cloud database. Therefore, our CAPEF flows same related policy language's architecture and structure. As discussed in the literature XACML is one of the good examples to extract our policies to its format. While Android system does not compile XACML language and all reviewed languages, our policies will be translated into java language to execute them, then will be extracted on different languages such as XML, JSON etc. Therefore, in order for our language to be compatible with other languages, we kept the same generic policy structure, objects and attributes applied by other languages as as shown in Table 2. Similar translation procedure will be applied when importing policies from other languages.

Among the values that can be assigned to attributes such as the names of applications, permissions, etc., we have defined symbols that allow us to simplify the rules, for example:

i ANY: it means no, for example a rental context, we do not need permission in this condition.

ii ALL: it means that we want to control all the permissions or all the applications it depends on the attributes used.

iii APPS: it means that we want to force the shutdown of an application.

iv API: that means we're going to apply the control on an API permission.

```
<?xml version="1.0" encoding="UTF-8"?>
<policy combine="deny-overrides" id="1" AUTHOR-KEY-CN="Mahdi" AUTHOR-KEY-FINGERPRINT="Mahdi">
   <target>
      <subject>
         <subject-match attr="id_ScreenShot" match="com.apps.TakeScreenShot" />
         <subject-match attr="id_BNC" match="com.apps.BNCbanque" />
      </subject>
   </target>
   <rule effect="deny">
      <condition>
         <ressources>
            <ressource>
               <ressource-match attr="APPS" subject-match="id_ScreenShot" match="ALL" />
            </ressource>
         </ressources>
         <contexts>
            <context>
               <context-match attr="UsedRessources" subject-match="id_BNC" match="android.permission.CAMERA" />
            </context>
         </contexts>
      </condition>
   </rule>
</policy>
```

Figure 5: An example of a security policy presented in the form of XML


```
{
    "@combine": "deny-overrides",
    "@id": "1",
    "@AUTHOR-KEY-CN": "Mahdi",
    "@AUTHOR-KEY-FINGERPRINT": "Mahdi",
    "target": {
        "subject": [
            {
                "@attr": "id_ScreenShot",
                "@match": "com.apps.TakeScreenShot"
            },
            {
                "@attr": "id_BNC",
                "@match": "com.apps.BNCbanque"
            }
        ]
    },
    "rule": {
        "@effect": "deny",
        "condition": {
            "ressources": {
                "ressource": {
                    "ressource-match": {
                        "@attr": "APPS",
                        "@subject-match": "id_ScreenShot",
                        "@match": "ALL"
                    }
                }
            },
            "contexts": {
                "context": {
                    "context-match": {
                        "@attr": "UsedRessources",
                        "@subject-match": "id_BNC",
                        "@match": "android.permission.CAMERA"
                    }
                }
            }
        }
    }
}
```


Figure 6: An example of a security policy presented in the form of JSON

The following scenario is established to extract CAPEF policies to communicate with other policy languages such as XML and JSON:

i Scenario: Prohibit launching the TakeScreenShot application that allows you to take automatic screenshots when the user opens the camera in his BankApp application to send a check.

Table 2: Generic policy description

Element	Description
Policy-set	Presents a table that groups the list of policies.
Policy	Presents the policy object that contains the" Target and" Rule Sub-objects, as well as the attributes:" Combine "which presents the role of the policy, the" AUTHOR-KEY-CN attribute the author identifier of the policy and the attribute AUTHOR-KEY-FINGERPRINT" presents the fingerprint key of the author of the policy.
Target	This is the object that contains the definition of the target applications to control.
Rule	It is the object that defines the security rule, the attribute" effect "presents the decision of the control to give or withdraw the authorization.
Condition	Contains the permissions to remove and the contexts.
Resource-match	Contains different attributes:" attr "which can be an application to block or an API permission," subject-match "contains the application to control and" match "contains the permission to remove.

ii Policy: if (CAMERA in [BNCApp]), then stop the application [TakeScreenShot].

Fig.5. shows the extraction of the above security policy scenario to XML and Fig.6. shows the extraction of the same scenario to JSON security policy.

6. Experimental results

This section presented the evaluation of our CAPEF and the application controller in terms of performance by analyzing: (1) the size of the enforced application after the instrumentation, 2) the execution time of the policy decision (3) The policy size due to the complexity of the applied rules and conditions.

6.1. Enforced Application Size

To measure the effect of the instrumentation method on the original size of the applications, we have instrumented a set of 109 applications using our rewriting framework. Table 3 shows a sample of eighteen applications, the original size and the new size after the instrumented. Indeed, this percentage represents the size of the code added during the control of APIs calls for each application individually

For all instrumented 109 applications, the average size added was 705 bytes, which is about 0.063% of the size of the original applications. Also, as shown in Fig.7, it is very clear that the size added is very small and will have a very small impact on the size of the original applications.

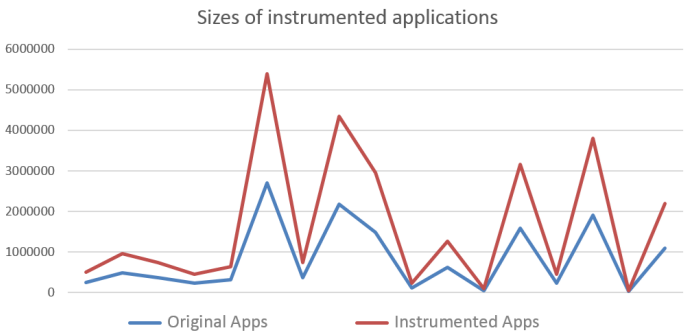


Figure 7: Average added size for 109 instrumented applications

6.2. Execution time of the policy decision

To calculate and evaluate the execution time of our defined policies, we have calculated the decision execution time for several context aware policies with different rules and conditions based on some selected scenarios. The following is a set of scenarios that has been chosen among many others used during our tests. These scenarios will be ranked in ascending order according to their level of complexity.

1. **Scenario 1**: Prohibit launching the TakeScreenShot application that allows you to take automatic screenshots when the user opens the camera in his BankApp application to send a Check.

   Policy: $\text{Deny}_{TakeScreenShot}$(app, per, c) ← (TakeScreenshot ∈ app.APIs) ∧ (per.resource==screen) ∧ (c.fgApp.class = banking)

2. **Scenario 2**: Prohibits the RecordAudioMedia application from recording when the user is making a phone call through the PhoneCall application.

   Policy: $\text{Deny}_{RecordAudioMedia}$ (app, per, c) ← (RecordAudioMedia ∈ app.APIs) ∧ (per.resource == microphone) ∧ (c.fgApp.class = (callPhone ∨ receivePhoneCall))

3. **Scenario 3**: Prohibit the FakeGPS application from changing the user's location when using one or more of these BankApp, Uber, and Google-Map applications.

   Policy: $\text{Deny}_{FakeGPS}$ (app, per, c) ← (FakeGPS ∈ apps.APIs) ∧ (per.resouce == (accessCoarseLocation ∧ accessFineLocation) ∧ (c.fgApp.Class = (BankApp ∧ UBER ∧ GoogleMap))

4. **Scenario 4**: Prohibition of the BankApp application to access the Internet or use the camera when the user is at TimHortons knowing that its longitude = 45.491318 and its latitude = -73.727987.

   Policy: $\text{Deny}_{internet \wedge camera}$ (app, per, c) ← ((internet ∧ camera) ∈ apps.APIs) ∧ (per.resource == (GPS = [45.491318, -73.727987]) ∧ (c.fgApp.Class = BankApp)

5. **Scenario 5**: When the user is at the meeting at ETS from 8am to 9am. Prohibit Facebook, Instagram and Gmail applications from accessing the Internet, the

Table 3: The size of applications before and after instrumentation

Application	Original (Bytes)	Instrumented (Bytes)	Size added (Bytes)	Percentage
Contact Identicons	246904	247965	603	0.24%
GPS tracker	22420823	22421668	845	0.0037%
Show web view	483839	484460	621	0.12%
Contact Search	368610	369278	668	0.18%
Contacts Widget	227386	228034	648	0.28%
Beta Updater for WhatsApp	321673	322448	775	0.24%
Contact loader	2701541	2702019	478	0.01%
Photo Manager	366100	366668	568	0.15%
Wi-Fi setup	2177239	2177747	508	0.02%
Time tracker	1477841	1478711	870	0.06%
Calender Trigger	119863	120732	869	0.72%
Calender Color	629361	630232	871	0.13%
Calender Import Export	45823	46772	949	2.07%
CamTimer	1580753	1581393	640	0.04%
OpenCamera	226585	227420	835	0.36%
Microphone	1905254	1905910	656	0.03%
SMS backup	26071	26984	913	3.50%

camera and the location. Prohibit Message application from receiving SMS and MMS. Also, Prohibit the recording feature of RecordAudio application.

Policy: Deny_{all} (app, per, c) ← ((Facebook ∧ Instagram ∧ Gmail∧ RecordAudioMedia ∧ SMS ∧ MMS) ∈ apps.APIs) ∧ (per.resouce ==(GPS = [45.491318, -73.727987] ∧ internet ∧ microphone ∧ phoneCall ∧ receiveCall)) ∧ (c.fgApp.Class = meeting) ∧ (c.time >= 8am ∧ c.time <=9am)

The decision execution time has been calculated for each policy individually as following:

i For the Policy 1 and Policy 2, the test results were fixed because the context does not vary when entering random test values. The execution time for the first policy is 116 ms and for the second policy is 234 ms.

ii For the policy 3, the context is related to three different running applications, but it remains fixed. The execution time for the whole policy is 307 ms.

iii For the policy 4, our context is the location, so the results were more or less close, but they vary according to the change in GPS values. In this case the execution time of the whole policy is 314 ms.

iv For the policy 5, two different contexts were used time and location. The average execution time for notifying each application also was calculated. For the Skype application the execution time is 549 ms, for the Messages application is 592 ms, for the Instagram application is 634 ms, for the Gmail application is 758 ms and for Facebook is 814. Also, the average execution time for the whole policy is 818 ms.

Fig.8, shows the different policies execution times according to the complexity for each policy. All calculations and testes where repeated several times to ensure accuracy. As a result, we have noticed that as more the policy becomes complex the execution time becomes bigger.

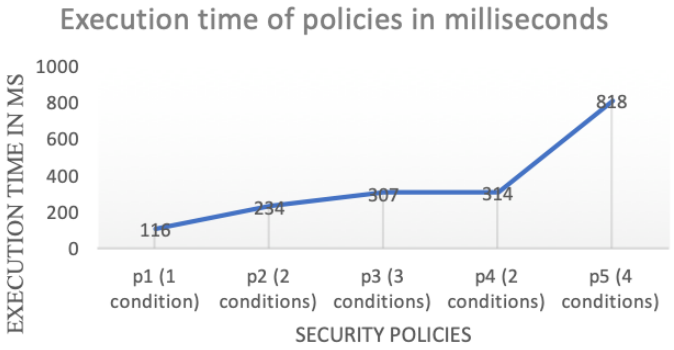


Figure 8: Policies execution times

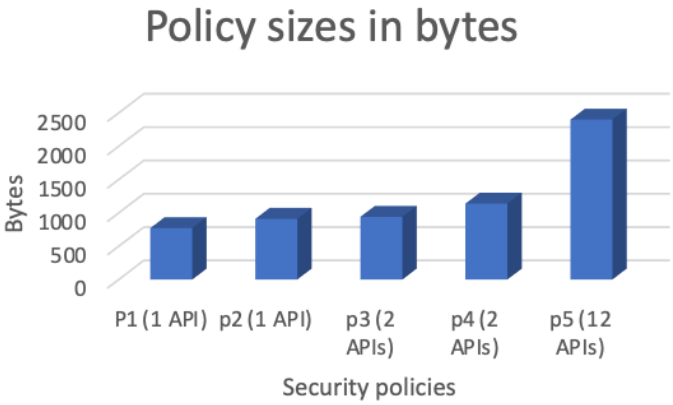


Figure 9: Policies sizes according to their complexities

6.3. Policy Size

The policy size is also changing due to the complexity of the applied rules and conditions. We have calculated the policy

sizes on the list of 109 enforced applications. Also, we took the same fife scenarios and their security policies mentioned above in the previous section to make our simulation. Fig. 9 shoes the progression of policy sizes according to their complexities.

7. Conclusion and Future Work

This work addressed problems related to context aware policies for Android applications as its one of the main targets of attackers. We, therefore developed CAPEF, which is a policy specification framework that enforces context-aware inter-app security policies to effectively describe users defined consents. Thorough experiments we have performed a study on the efficiency of CAPEF with respect to the size and execution time of the enforced applications. The evaluation results demonstrated the feasibility of our framework and the effectiveness of our policy specification language in enforcing complex context-aware policies on different Android applications.

In the future, we are planning to improve our model using different ML techniques for varying IoT smart environments. Furthermore, we will implement a security framework that is capable of data security and access control by encrypting all sensitive data and making it available only for the authorized service providers according to the pre-defined context-aware policies.

References

[1] J. Maring, "Android central", Online[Access 12/07/2022] urlhttps://www.androidcentral.com/google-removed-over-700000-malicious-apps-play-store-2017, 2018.

[2] I. Rathore, "Google gets rid of these 16 apps having millions of downloads", Online[Access 15/09/2022] https://dazeinfo.com/2022/10/25/ google-removes-apps-that-have-affected-20-million-android-users-worldwide/, 2022.

[3] "Android developers", Online[Access 02/01/2022]urlhttps://developer.android.com /guide/topics/manifest/ manifest-intro.

[4] V. Arena, V. Catania, G. La Torre, S. Monteleone, F. Ricciato, "Securedroid: An android security framework extension for context-aware policy enforcement", "Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on", pp. 1–8, IEEE, 2013, doi:10.1109/PRISMS.2013.6927185.

[5] M. Nauman, S. Khan, X. Zhang, "Apex: extending android permission model and enforcement with user-defined runtime constraints", "Proceedings of the 5th ACM symposium on information, computer and communications security", pp. 328–332, 2010, doi:10.1145/1755688.1755732.

[6] Y. Zhou, X. Zhang, X. Jiang, V. W. Freeh, "Taming information-stealing smartphone applications (on android)", "International conference on Trust and trustworthy computing", pp. 93–107, Springer, 2011, doi:10.1007/978-3-642-21599-5_7.

[7] P. Hornyack, S. Han, J. Jung, S. Schechter, D. Wetherall, "These aren't the droids you're looking for: Retrofitting android to protect data from imperious applications", "Proceedings of the 18th ACM Conference on Computer and Communications Security", CCS '11, p. 639–652, Association for Computing Machinery, New York, NY, USA, 2011, doi:10.1145/2046707.2046780.

[8] D. Feth, A. Pretschner, "Flexible data-driven security for android", "Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on", pp. 41–50, IEEE, 2012, doi:10.1109/SERE.2012.14.

[9] R. Xu, H. Saidi, R. Anderson, "Aurasium: Practical policy enforcement for android applications", "21st USENIX Security Symposium (USENIX Security 12)", pp. 539–552, USENIX Association, 2012, 21st USENIX Security Symposium ; Conference date: 08-08-2012 Through 10-08-2012.

[10] J. Jeon, K. K. Micinski, J. A. Vaughan, A. Fogel, N. Reddy, J. S. Foster, T. Millstein, "Dr. android and mr. hide: Fine-grained permissions in android applications", "Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices", SPSM '12, p. 3–14, Association for Computing Machinery, New York, NY, USA, 2012, doi:10.1145/2381934.2381938.

[11] B. Davis, B. Sanders, A. Khodaverdian, H. Chen, "I-arm-droid: A rewriting framework for in-app reference monitors for android applications", *Mobile Security Technologies*, vol. 2012, no. 2, p. 17, 2012.

[12] B. Davis, H. Chen, "Retroskeleton: Retrofitting android apps", "Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services", MobiSys '13, p. 181–192, Association for Computing Machinery, New York, NY, USA, 2013, doi:10.1145/2462456.2464462.

[13] P. von Styp-Rekowsky, S. Gerling, M. Backes, C. Hammer, "Idea: Callee-site rewriting of sealed system libraries", J. Jürjens, B. Livshits, R. Scandariato, eds., "Engineering Secure Software and Systems", pp. 33–41, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[14] X. Zhang, A. Ahlawat, W. Du, "Aframe: Isolating advertisements from mobile applications in android", "Proceedings of the 29th Annual Computer Security Applications Conference", ACSAC '13, p. 9–18, Association for Computing Machinery, New York, NY, USA, 2013, doi:10.1145/2523649.2523652.

[15] P. Pearce, A. P. Felt, G. Nunez, D. Wagner, "Addroid: Privilege separation for applications and advertisers in android", "Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security", ASIACCS '12, p. 71–72, Association for Computing Machinery, New York, NY, USA, 2012, doi:10.1145/2414456.2414498.

[16] S. Shekhar, M. Dietz, D. S. Wallach, "Adsplit: Separating smartphone advertising from applications", "Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)", pp. 553–567, 2012, doi:10.48550/arXiv.1202.4030.

[17] M. Zhang, H. Yin, "Efficient, context-aware privacy leakage confinement for android applications without firmware modding", "Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security", ASIA CCS '14, p. 259–270, Association for Computing Machinery, New York, NY, USA, 2014, doi:10.1145/2590296.2590312.

[18] Y. Falcone, S. Currea, "Weave droid: aspect-oriented programming on android devices: fully embedded or in the cloud", "Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering", pp. 350–353, 2012, doi:10.1145/2351676.2351744.

[19] O. Riganelli, D. Micucci, L. Mariani, "Controlling interactions with libraries in android apps through runtime enforcement", *ACM Trans. Auton. Adapt. Syst.*, vol. 14, no. 2, 2019, doi:10.1145/3368087.

[20] M. Alhanahnah, Q. Yan, H. Bagheri, H. Zhou, Y. Tsutano, W. Srisa-An, X. Luo, "Dina: Detecting hidden android inter-app communication in dynamic loaded code", *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2782–2797, 2020, doi:10.1109/TIFS.2020.2976556.

[21] M. Grace, M. Sughasiny, "Behaviour analysis of inter-app communication using a lightweight monitoring app for malware detection", *Expert Systems with Applications*, vol. 210, p. 118404, 2022, doi:https://doi.org/10.1016/j.eswa.2022.118404.

[22] A. Developers, "Preparing for the android privacy sandbox beta", Online[Access 15/12/2022]urlhttps://android-developers.googleblog.com/2022/11/preparing-for-android-privacy-sandbox-beta.html , 2022.

[23] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, "Role-based access control models", *Computer*, vol. 29, no. 2, pp. 38–47, 1996, doi:10.1109/2.485845.

[24] OASIS, "Oasis extensible access control markup language (xacml)", Online[Access 02/05/2017]urlhttp://www.oasis-open.org/committees/xacml, 2011.

[25] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones", *ACM Trans. Comput. Syst.*, vol. 32, no. 2, 2014, doi:10.1145/2619091.

[26] W. Zhou, X. Zhang, X. Jiang, "Appink: Watermarking android apps for repackaging deterrence", ASIA CCS '13, p. 1–12, Association for Computing Machinery, New York, NY, USA, 2013, doi: 10.1145/2484313.2484315.

SAAD INSHI is currently pursuing his PhD in software engineering from École de technologie supérieure, University of Quebec, Montreal, Canada and completed his MASc degree in Information Systems Security from Concordia University, Montreal.

His research interests includes Android and IoT Privacy and security. He is also interested in Context aware privacy and security of devices.

MAHDI ELARBI has completed Masters from École de technologie supérieure, University of Quebec, Montreal, Canada. He is currently working as a senior Software Developer in Montreal.

His research interests includes Android and IoT security.

RASEL CHOWDHURY is pursuing his PhD in software engineering and completed his MSc degree in Information Technology Engineering from École de technologie supérieure, University of Quebec, Montreal, Canada.

His research interests includes Cloud Computing, Cloud Native orchestration, security and privacy of IoT, IoE and IoV.

HAKIMA OULD-SLIMANE is currently a professor at the Département de Mathématiques et d'Informatique, Université du Québec à Trois-Rivières, Trois-Rivières, Canada. She obtained her Ph.D. degree in Computer Science from Laval University, Québec, Canada.

Her research interests include mainly: information security, cryptography, preserving data privacy in smart environments, reliability of collaborative computing and formal methods.

CHAMSEDDINE TALHI is currently a Full Professor with the Department of Software Engineering and IT, École de Technologie Supérieure, University of Quebec, Montreal, Quebec, Canada.

He is leading a research group that investigates efficient security mechanisms for smartphone, IoT, edge and cloud infrastructures. His current research interests include cloud native telco services management and security, DevOps security, and federated learning for mobile cloud and IoT.

Received: 10 November, 2022, Revised: 03 January 2023, Accepted: 04 January 2023, Online: 28 January, 2023

DOI: https://doi.org/10.55708/js0201003

A Tunable Dual-mode SIW Cavity Based Bandpass Filter with Wide Upper Stopband Characteristics

Md. Atiqur Rahman*, Pankaj Sarkar

Department of Electronics & Communication Engineering, School of Technology, North-Eastern Hill University, Shillong, 793022, India
*Corresponding author: Md. Atiqur Rahman, +91-7005468917 & atiqurece@gmail.com

ABSTRACT: A new approach to design a bandpass filter using substrate integrated waveguide (SIW) topology is presented here for 5G applications. The aim of the design is to produce a dual mode passband characteristic with wide upper stopband behaviour, centred at 4.7 GHz. Four identical Stepped Impedance Resonator (SIR) slots are etched into the top surface of the SIW cavity for the proposed filter structure. The SIR slots aid in reducing the cavity's resonant frequency and to generate the dual mode passband characteristics. The SIR slots also mitigate the higher modes in the SIW cavity which helps to accomplish a wide upper stopband response. In order to improve selectivity, the structure is further modified by introducing two E shaped resonator slots on the ground plane to produce two transmission zeros at 3.9 GHz and 6.2 GHz. Tunable characteristic is achieved by loading two surface mount varactor diodes diagonally on the top of the proposed structure. By suitably applying the bias voltage, the center frequency of the passband is tuned over a range of 600 MHz. The developed filter is fabricated in order to verify the simulated and measured results.

KEYWORDS: Substrate Integrated Waveguide Cavity, Bandpass Filter, Stepped Impedance Resonator slot, E-Shaped Resonator, Wide upper stopband, 5G Application.

1. Introduction

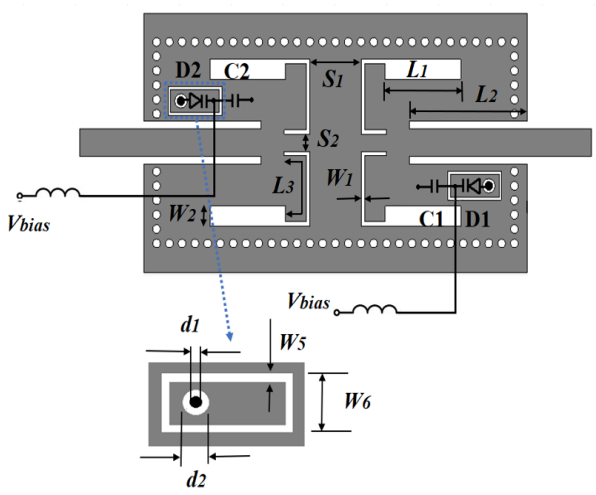
Substrate Integrated Waveguide (SIW) technology has attracted a great deal of attention in the research community due to its advantages such as low cost, light weight, ease of fabrication, minimal radiation loss, and good power handling. As a result, SIWs have demonstrated their viability as an innovation and continue to have significant potential as a crucial component of planer microwave circuits, such as highly selective filters, Voltage-Controlled Oscillators (VCOs) and antennas [1-3]. In [4], a compact SIW filter is reported with an E-shape slot etched on the topmost surface to reduce the filter's resonant frequency. In [5], a SIW bandpass filter is made using double-sided loading approach defective ground structure (DGS) bandpass filter (BPF). SIW based bandpass filter based on upper stopband performance are reported in [6-7].

One of our very recent developments shows the utilization of SIR slots on the SIW cavity to develop the dual-mode BPF [8]. A HMSIW doublet was created by employing the rectangular cavity's TE_{102} and TE_{301} modes as resonant, and TE_{101} as a non-resonant mode reported in [9]. Several SIW-based tunable filter has been investigated by various researchers [10-12]. A tunable SIW dual mode dual-band filter using perturbing metalized via hole at the middle of the cavity is reported in [10]. In [11] a constant bandwidth highly selective tunable dual-mode BPF is investigated. A stub-loaded capacitor tunable dual-band HMSIW has been reported in [12].

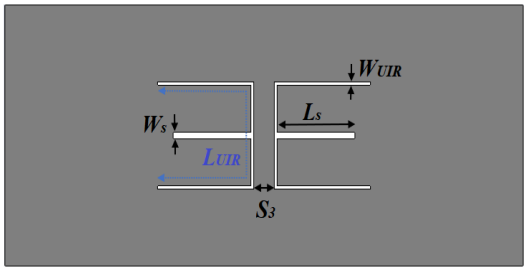
In this manuscript, analytical and synthesis procedure is presented to implement the dual mode BPF for n79 band (4.4-5.0 GHz) of 5G New Radio (NR) application [13]. A rectangular cavity is designed in conjunction with four SIR slots to lower the resonating frequency. Additionally, two shaped-shaped resonators are introduced in the ground plane in order to improve the selectivity, and the upper stopband characteristic of the proposed filter. Finally, the proposed structure is tuned by loading two surface-mounted varactor diodes with two capacitors diagonally. For the design purpose, 1.00 mm thick FR4 substrate is employed. EM simulation is performed using CST Microwave Studio.

2. Filter Design

Top and the bottom views of the proposed tunable dual-mode SIW-based BPF are displayed in Figure 1(a) and Figure 1(b).

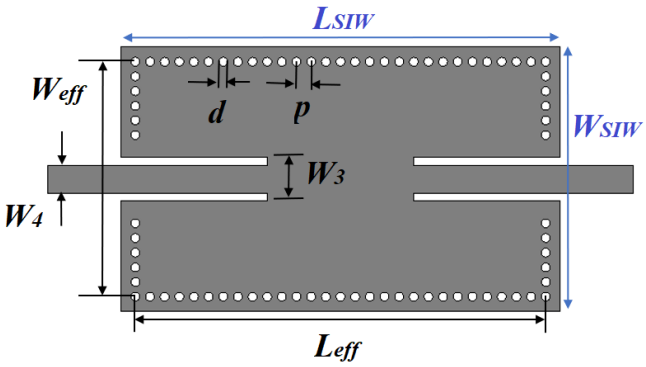


(a)

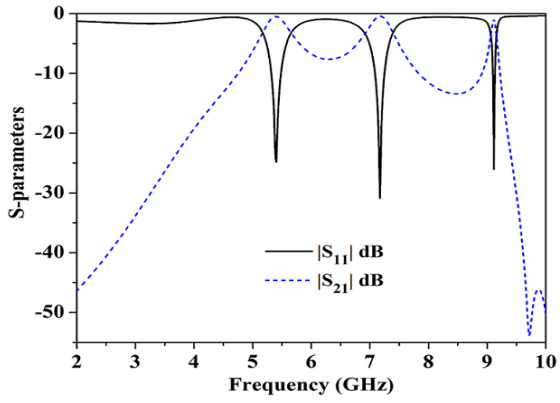


(b)

Figure 1: Proposed tunable bandpass filter layout and necessary tuning arrangements (a)Top view with L_1=7, L_2 =9.2 , L_3 =9.3 ,W_1=0.3 ,W_2=1.4 ,S_1=5.6 , S_2=1.2, L_4= 4.2, W_5= 0.2, W_6= 2, d_1= 0.6, d_2= 1.0 (*all dimensions in mm*). (b) Bottom view with L_S=6.1, L_{UIR}=21.6, W_S=0.3, W_{UIR}=1.4, S_3=5.6 (*all dimensions in mm*).



(a)



(b)

Figure 2: (a) SIW cavity layout with L_{eff}= 28, L_{SIW}= 30, W_3=3, W_4=1.9, W_{eff} = 14, W_{SIW} =16, p=1, d = 0.6 (*all the dimensions in mm*). (b) SIW cavity's simulated S-parameters.

As shown in Figure 2(a), a SIW cavity is initially designed. The fundamental frequency of resonance of the proposed cavity is designed at 5.3 GHz [1]. The cavity resonance is kept a little high to minimize the area requirement. In Figure 2(b) the S-parameters of the simulated SIW cavity are illustrated. It can observe that the fundamental frequency of the resonator is 5.3 GHz. Up to 10 GHz, there are two spurious frequencies centered at 7.1 GHz and 9.1 GHz.

On top of the SIW cavity, stepped impedance resonators (SIRs) are placed to achieve dual-mode features and mitigate spurious frequency ranges. Inset in Figure 3 highlights the open-ended SIR's configuration. The SIR is made up of electrical sections Z_1 and Z_2 with corresponding electrical lengths of θ_1 and θ_2, and high and low impedance portions Z_1 and Z_2, respectively. An essential factor in modifying the SIR features is R_Z = (Z_2/Z_1). The SIR input admittance is derived as:

$$Y_{in} = jY_2 \frac{Z_2 + Z_1 \cot\theta_1 \tan\theta_2}{Z_1 \cot\theta_1 - Z_2 \tan\theta_2} \quad (1)$$

The resonance condition is determined considering Y_{in}=0. Figure 3 plots the ratio of normalized first spurious frequency (f_1) and fundamental frequency (f_0) for various impedance ratios (R_Z), to easily extract the design parameters. To achieve the dual mode characteristics, fundamental resonant frequency is maintained at 4.5 GHz. The first spurious of SIR is predicted to be at 10.8 GHz, for a spurious free response up to 10 GHz. For fundamental frequency and the first spurious , the SIR has an impedance ratio of 0.57. Z_2 has a 60 Ω impedance, and its corresponding electrical length, θ_2 is 68^0. The high impedance section's computed impedance Z_1 is 113Ω with an electrical length of 88^0. The dimensions of low impedance part has 7 mm in length, 1.4 mm in width, and for high impedance part are 9.3 mm and 0.3 mm, respectively.

Finally, the topmost surface of the cavity is etched with the SIR structure. For symmetry reasons, four SIRs are etched into the SIW cavity as, displayed in the inset of Figure 4(a). The classical filter design methods are adopted [14] to meet the design specification for n79 band (4.4-5.0 GHz), of 5G New Radio (NR). The circuit's coupling coefficient (k) and external quality factor (Q_e) components of a prototype lowpass filter is determined in order to develop the proposed filter. The Q_e and k for any designed filter can be calculated as provided in [13]. Figure 4(a) shows the Q_e and k for different separations S_1. It can be observed that the higher value of Q_e can be obtained by increasing the S_1. The value of k can also be significantly controlled by S_1. It can be inferred that the higher value of k can be achieved by reducing S_1. To facilitate the design procedure, the value of Q_e and k is required to find for the

proposed filter. For the required passband from 4.4 GHz to 5.0 GHz the value of Q_e is 10.2 whereas the calculated value of k is 0.075. To accomplish the required Q_e and k the S_1 is determined to be 4.2 mm. The value of S_1 is revised further and selected to be 4.0 mm.

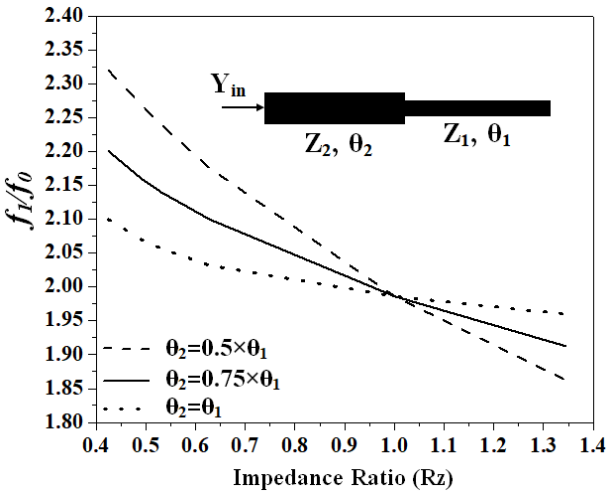
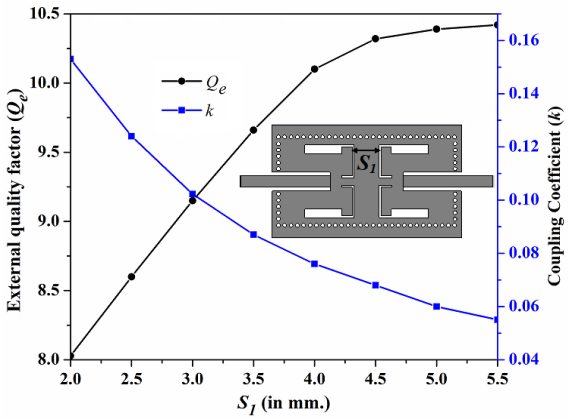
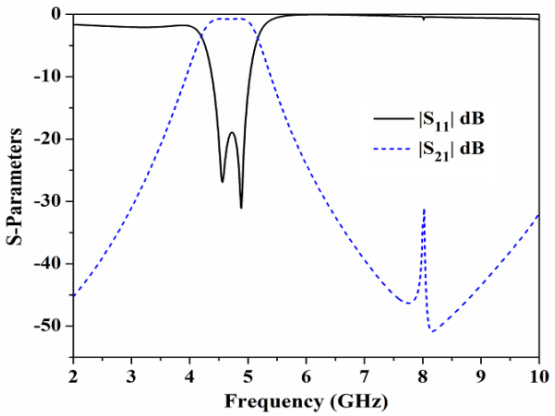


Figure 3: Ratio of first spurious to fundamental frequency vs impedance ratio plot of SIR.



(a)



(b)

Figure 4: (a) For various values of S_1, the coupling coefficient (k) and the external quality factor (Q_e). (b) The dual mode filter's frequency response employing SIR slots.

Figure 4 (b) depicts the simulated filter S-parameters. It is clear that the suggested filter results in a dual-mode characteristic with a passband ranging from 4.4 GHz upto 5 GHz. Through the passband, the S_{21} is better than -0.3 dB and the S_{11} value is less than -19.0 dB. Additionally, it can be seen that the SIR's presence suppresses the spurious bands. The upper stopband response is satisfactory with attenuation levels greater than 30 dB are achieved up to 10 GHz.

Figure 4(b) inferred that the selectivity of the filter is poor. Therefore, to increase the selectivity, two E-shaped resonators are introduced in the ground plane. The basic -shaped stub structure is displayed in inset of Figure 5. A uniform impedance resonator (UIR) with electrical length θ_{UIR} and admittance Y_1 is used to realize the resonator. A stub of electrical length θ_S and admittance Y_S is loaded into the center of the resonator. The input admittance is derived as follows for even and odd modes.

$$Y_{in,\,odd} = -jY_1\cot(\theta_{UIR}/2) \tag{2}$$

$$Y_{\text{in, even}} = jY_1\frac{Y_S\tan(\theta_S)+2Y_1\tan(\theta_{UIR}/2)}{2Y_1-Y_S\tan(\theta_S)\tan(\theta_{UIR}/2)} \tag{3}$$

The resonance condition can be determined by setting $Y_{in,odd}$=0, and $Y_{in,even}$=0. Resonating modes f_o and f_e are extracted by assuming Y_1=Ys/2. Figure 5 shows the normalized odd and even modes of resonant frequency for different values of L_R and L_S. The E-shaped resonator is designed to form two modes at 4.0 GHz and 6.0 GHz. From the plot, it can be observed that the f_o is fully depends on L_R whereas the f_e can be controlled by L_R and L_S. The calculated value of L_R and L_S is tuned further to improve the performance. The resonating frequencies are chosen to improve the selectivity. For L_R and L_S, optimal values are 10.5 mm and 6.0 mm, respectively. In order to generate a considerable degree of attenuation at the appropriate frequency, the inter-resonator spacing (S_3) is adjusted.

2.1. Reconfigurable Bandpass Filter Design

In order to achieve the tunable characteristics, the proposed dual-mode BPF is loaded with two surface-mounted varactor diodes diagonally. Figure 1 depicted the proposed tunable bandpass filter where two SMV (1232-079LF and two DC blockers (C0603C330K5RACTU) are used. The anode terminal of the varactor diode is connected to the ground using a metallic post. The cathode terminal is landed on a rectangular island where bias voltage is applied. The diodes D1 and D2 are connected to the cavity through the two DC blockers C1 and C2 respectively. Through a 27 nH inductor, the bias voltage is applied to the varactor diode.

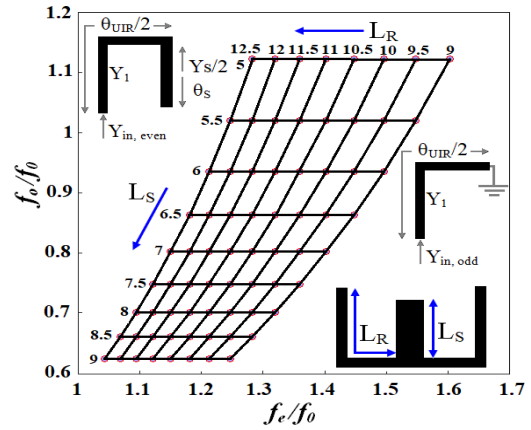
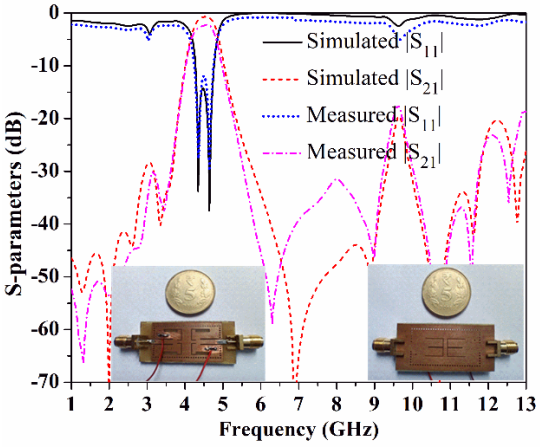
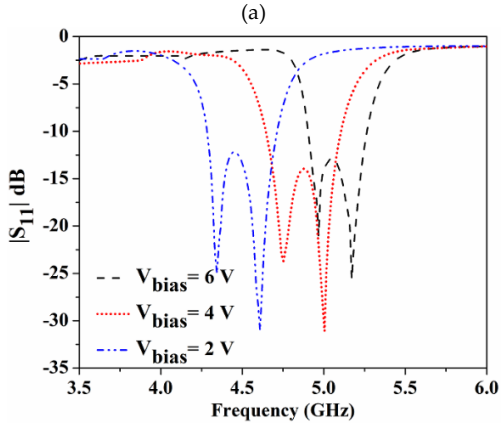


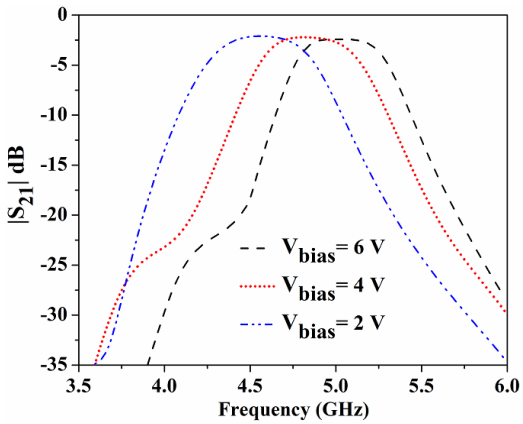
Figure 5: Normalized even and odd mode resonating frequencies for different values of L_R and L_S.



(a)



(b)



(c)

Figure 6: (a) Comparison of the proposed filter's S-parameters as simulated and measured. S-parameters simulations at various bias voltages (b) $|S_{11}|$ dB (c) $|S_{21}|$ dB.

3. Measured Results and Discussion

The fabricated prototype is displayed in Figure 6(a) as inset. The EM-simulated and measured S-parameters are compared in Figure 6(a). It can be seen that with the bias voltage V_{bias}=3V, the proposed filter gives a measured passband from 4.42 to 5.03 GHz. The measured S_{11} is less than -12.0 dB throughout the passband, while the measured S_{21} is better than -2.1 dB. Further observations include the suppression of spurious bands and the presence of two transmission zeros at frequencies of 3.85 GHz and 6.35 GHz. This improves the selectivity of the proposed filter. Three more number of transmission zeroes can be observed at 10.8 GHz, 11.7 GHz, and 12.6 GHz which increases the stopband range. More than 17 dB attenuation level is witnessed up to 13 GHz. Figure6(b) and 6(c) shows the $|S_{11}|$ and $|S_{21}|$ simulated results of the proposed tunable bandpass filter. By varying, the bias voltage of the varactor diode, which ranges from 2 to 6 V, the filter's center frequency can be tuned. Where can be observed, the passband center frequency can be moved from 4.5 GHz to 5.1 GHz as the reverse bias voltage rises. Over a bandwidth of 600 MHz structure is tuned. Throughout the tuning range, S_{11} is below -12 dB, and the S_{21} is better than -2.1 dB with excellent selectivity. Overall size of the filter is 30×18 mm². A comparative analysis is presented in Table 1 with previously published works. It can be observed that the proposed filter has better insertion loss compared to the work reported in [9] and [12]. The proposed filter has accomplished better stopband range and better fractional bandwidth compared to the filters presented in [7], [9], [10] and [12]. The filter structure exhibits a compact size compared to the filter reported in [7], [9] and [10]. The skirt factor, which is defined as the ratio of the passband's 3 dB bandwidth to its 20 dB bandwidth, is presented in order to explain selectivity. The skirt factor is 0.44 for the proposed filter which better compared to the filters presented in [7], [9], [10] and [12].

4. Conclusion

This manuscript presents a novel tunable dual-mode bandpass filter using SIW cavity. Etching SIRs into the top surface of the SIW cavity results in the dual-mode passband and a wide upper stopband performance. E-shaped resonators in the ground plane improve the selectivity. The resonating structures are properly analyzed and the resonating frequencies are determined. The tunable characteristic is achieved by employing two varactor diodes with good return loss and wide tuning range. The filter has compact size, low insertion loss, excellent selectivity, and wide upper stopband characteristics which are useful for modern communication systems.

Table 1: Performance comparison with some SIW based bandpass filter

Ref.	Response	Tunable	Center Frequency (f_0 GHz)	FBW (%) Fractional Bandwidth	RL(dB) Return Loss	IL(dB) Insertion Loss	Skirt Factor	Stopband frequency (a× f_0)	Stopband attenuation (dB)	Size ($\lambda_g \times \lambda_g$) ($\lambda_g^2$)
[7]	SIW BPF	No	13/13.2	4.6/4.5	15/10	1.7/1.5	0.4/0.35	($2f_0$) /($2.2 f_0$)	20/20	0.9316
[9]	Dual-Mode BPF	No	10	5.3	18	2.4	0.34	1.05 f_0	30	1.75
[10]	Dual-mode Dual-Band BPF	Yes	17/19.36	2.01/4.1	17	2.1/1	0.38/0.18	($1.05f_0$) /($1.13 f_0$)	20/20	2.62
[12]	Dual-Band BPF	Yes	2.25/4.5	13.33/8.8	15/17	2.33/3.38	0.25/0.25	($1.42f_0$) /($1.33 f_0$	20/20	0.04
This work	Dual-Mode BPF with wide upper stopband characteristics	Yes	4.7	14.89	12	2.1	0.43	(2.85 f_0)	17	0.44

λ_g is the guided wavelength derived at the passband's center frequency passband, RL stands for Return Loss, IL for Insertion Loss, and FBW for Fractional Bandwidth.

References

[1] D. Deslandes and K. Wu, "Single-substrate integration technique of planar circuits and waveguide filters," *IEEE Transactions on Microwave Theory and Techniques*, vol. 51, no. 2, pp. 593-596, 2003, doi: 10.1109/TMTT.2002.807820.

[2] A. Parameswaran and S. Raghavan, "Novel siw dual mode band pass filter with high skirt selectivity," *2nd International Conference for Convergence in Technology (I2CT)*, 2017, pp. 189-191, doi: 10.1109/I2CT.2017.8226118.

[3] M. Almalkawi, M. Westrick, V. Devabhaktuni, M. Alam, L. Zhu and J. Deng, "Design of a dual-band dual-mode substrate integrated waveguide filter with symmetric transmission zeros," *IEEE Applied Electromagnetics Conference (AEMC)*, 2011, pp. 1-3, doi: 10.1109/AEMC.2011.6256872.

[4] H. Zhang, W. Kang and W. Wu, "Miniaturized Dual-Band SIW Filters Using E-Shaped Slotlines With Controllable Center Frequencies," *IEEE Microwave and Wireless Components Letters*, vol. 28, no. 4, pp. 311-313, 2018, doi: 10.1109/LMWC.2018.2811251.

[5] S. Xu, K. Ma, F. Meng and K. S. Yeo, "Novel Defected Ground Structure and Two-Side Loading Scheme for Miniaturized Dual-Band SIW Bandpass Filter Designs," *IEEE Microwave and Wireless Components Letters*, vol. 25, no. 4, pp. 217-219, 2015, doi: 10.1109/LMWC.2015.2400916.

[6] S. Wang, D. Zhang, Y. Zhang, L. Qing and D. Zhou, "Novel Dual-Mode Bandpass Filters Based on SIW Resonators under Different Boundaries," *IEEE Microwave and Wireless Components Letters*, vol. 27, no. 1, pp. 28-30, 2017, doi: 10.1109/LMWC.2016.2629963.

[7] D. Jia, Q. Feng, Q. Xiang and K. Wu, "Multilayer Substrate Integrated Waveguide (SIW) Filters With Higher-Order Mode Suppression," *IEEE Microwave and Wireless Components Letters*, vol. 26, no. 9, pp. 678-680, 2016, doi: 10.1109/LMWC.2016.2597222.

[8] M. A. Rahman and P. Sarkar, "A Novel Compact Dual-Mode Substrate Integrated Waveguide Cavity based Bandpass Filter for WLAN Applications," *International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 059-061, doi: 10.1109/ComPE49325.2020.9200038.

[9] F. Zhu, G. Q. Luo, Z. Liao, X. W. Dai and K. Wu, "Compact Dual-Mode Bandpass Filters Based on Half-Mode Substrate-Integrated Waveguide Cavities," *IEEE Microwave and Wireless Components Letters*, vol. 31, no. 5, pp. 441-444, 2021, doi: 10.1109/LMWC.2021.3066569.

[10] M. F. Abbas, and A. J. Salim, "A New Tunable Dual-Mode Dual-Band Square Cavity SIW Bandpass Filter," *Progress In Electromagnetics Research C*, vol. 118, pp. 113-123, 2022, doi:10.2528/pierc21120306

[11] M. Abdelfattah, R. Zhang and D. Peroulis, "High-Selectivity Tunable Filters With Dual-Mode SIW Resonators in an L-Shaped Coupling Scheme," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 12, pp. 5016-5028, 2019, doi: 10.1109/TMTT.2019.2944365.

[12] C. X. Zhou, C. M. Zhu and W. Wu, "Tunable Dual-Band Filter Based on Stub-Capacitor-Loaded Half-Mode Substrate Integrated Waveguide," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 1, pp. 147-155, 2017, doi: 10.1109/TMTT.2016.2613053.

[13] 5G NR specifications, document TS 38.101-1 V15.4.0 3GPP Release15, Dec. 2018.

[14] J. S. G. Hong, and M. J. Lancaster, "*Microstrip filters for RF/microwave applications*,"John Wiley & Sons, 2004.

Md. Atiqur Rahman received his B.Tech degree in Electronics and Communication Engineering from North Eastern Hill University-Shillong in 2015 and M.Tech degree in Electronics and Communication Engineering from North Eastern Hill University-Shillong in 2017. Presently he is pursuing his Ph.D. from North Eastern Hill University- Shillong. His research interest lies in the area of microwave passive circuit design, antenna. Several of his conference papers received the best paper award.

Pankaj Sarkar received his M.Tech degree from Burdwan University and Ph.D. from Jadavpur University in the year of 2009 and 2016, respectively. He worked one year in Space Applications Center-Ahmedabad as a trainee for M. Tech project entitled as "Design of MMIC Mixer at 50-60 GHz". He initiated his teaching carrier from ITER (Siksha "O" Anusandhan University-Bhubaneswar), after that he served Sikkim Manipal Institute of Technology and National Institute of Technology-Sikkim. Presently he is an Assistant Professor in Electronics and Communication Engineering Department of North-Eastern Hill University (A Central University)-Shillong.

He has more than 50 publications in various National/International journals and conferences. He is the reviewer of various journals such as IEEE Transactions on Microwave Theory and Techniques, IEEE Transactions on Industrial Electronics, IEEE Microwave and Wireless Components Letters, Electronics Letters, IET Microwaves, Antennas and Propagation, Progress in Electromagnetics Research (PIER), Microwave and Optical Technology letters and so forth. His research interest lies in the area of microwave passive circuit design, metamaterials, MMIC, antenna. He has been a member of various program committee for several international conferences. He chaired various technical session for the international conferences.