Monitoring for Reliable and Secure Power Management Integrated Circuits via Built-In Self-Test

by

Pragya Malakar

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved July 2019 by the
Graduate Supervisory Committee:

Jennifer Kitchen, Chair
Sule Ozev
John Brunhaver

ARIZONA STATE UNIVERSITY

August 2019

ABSTRACT

Power management circuits are employed in most electronic integrated systems, including applications for automotive, IoT, and smart wearables. Oftentimes, these power management circuits become a single point of system failure, and since they are present in most modern electronic devices, they become a target for hardware security attacks. Digital circuits are typically more prone to security attacks compared to analog circuits, but malfunctions in digital circuitry can affect the analog performance/parameters of power management circuits. This research studies the effect that these hacks will have on the analog performance of power circuits, specifically linear and switching power regulators/converters. Apart from security attacks, these circuits suffer from performance degradations due to temperature, aging, and load stress. Power management circuits usually consist of regulators or converters that regulate the load's voltage supply by employing a feedback loop, and the stability of the feedback loop is a critical parameter in the system design. Oftentimes, the passive components employed in these circuits shift in value over varying conditions and may cause instability within the power converter. Therefore, variations in the passive components, as well as malicious hardware security attacks, can degrade regulator performance and affect the system's stability. The traditional ways of detecting phase margin, which indicates system stability, employ techniques that require the converter to be in open loop, and hence can't be used while the system is deployed in-the-field under normal operation. Aging of components and security attacks may occur after the power management systems have completed post-production test and have been deployed, and they may not cause catastrophic failure of the system, hence making them difficult to detect. These two issues of component variations and security attacks can be detected during normal operation over the product lifetime, if the frequency response of the power converter can be monitored in-situ and in-field. This work presents a method to monitor the phase margin (stability) of a power converter without affecting its normal mode of operation by injecting a white noise/ pseudo random binary sequence (PRBS). Furthermore, this work investigates the analog performance parameters, including phase margin, that are affected by various digital hacks on the control circuitry associated with power converters. A case study of potential hardware attacks is completed for a linear low-dropout regulator (LDO).

ACKNOWLEDGMENTS

I sincerely thank Prof. Jennifer Kitchen for giving me the opportunity to work with her. I am very grateful for her constant support, encouragement, patience and valuable guidance. I would also like to thank professor Sule Ozev for showing interest in my work and providing me with valuable inputs. I am grateful to professor John Brunhaver for being a part of my defense committee and giving me valuable feedback about my work.

In addition, I would like to thank Prof. Bertan Bakkaloglu and Prof. David Allee for teaching the Analog design courses from which I developed my interest in analog circuits.

I would also like to thank Shrikant Singh for his help with Analog design and constant encouragement. I also thank all my colleagues at ASU for helping me grow and their constant support.

Finally, my deep and sincere gratitude to my family for their continuous and unparalleled love, help and support. I am grateful to my brother, Jhankar Malakar who has always helped me understand the soul of Analog Design, given me feedback from an industrial perspective and has always been there through thick and thin.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Figure Page

Figure Page

LIST OF PLOTS

Plot Page

CHAPTER 1

INTRODUCTION

Power management is omnipresent in the majority of the electronic systems, as it controls the delivery of power throughout the system and optimizes efficiency. Power Management integrated Chip (PMIC) are a class of integrated circuits that perform various power distribution, regulation, and/or power control for various sub-systems. They are essential to maximizing battery life in mobile devices that are packing in more features and higher performance with the intent of longer use between charging the device. Examples include power regulation of handset batteries, solar power distribution for satellite communications electronics, low-power management, control in IoT, wearable electronics etc. The PMIC market is expected to witness high growth with estimated growth from USD 20.09 billion in 2015 to USD 34.86 billion by 2022 [7]. The growing number of these PMICs in almost all electronics systems makes it a target sub-system for hardware attacks as the PMIC(s) is a single point of failure for many electronic systems because the PMIC typically regulates power for multiple electronic loads. Therefore, there is a need to develop reliably operating PMICs that maintain their performance specifications over the lifetime of the product. Any breach or failure that occurs during in-field operation of the device won't be caught in the post-production testing and a method is needed to monitor these power management circuits in the field, without disturbing the normal mode of operation. The objective of this thesis is to study the effect that security breaches or aging of components will have on the reliable operation of a PMIC, which indicates the motivation to monitor them in-field. The thesis also investigates a method for monitoring their performance without affecting their normal mode of operation. The outline is as follows, chapter 1 provides a brief introduction to the DC-DC converters, explains their utility in modern-day electronics, and the importance of reliable operation of these systems. The 2nd chapter outlines the method to monitor the performance of a switching power converter for reliable operation over the lifetime of the product. Lastly, the 3rd chapter studies the effect of security breaches on another class of power converters and a method to monitor the same.

1.1 PMIC Application

A typical PMIC (Power Management Integrated Chip) has multiple voltage regulators, these are supplied by the battery. Figure 1 is a die photograph of a PMIC for mobile application which labels the different parts a PMIC may have. Applications for PMICs include IoT, automotive, industrial and consumer products, also used widely in smartphones and wearable devices. These devices may integrate several PMICs that dynamically manage battery life and usage. Along with battery technology, battery management is one of the major factors contributing to consumer satisfaction. PMICs are used in portable electronic devices that are primarily supplied with power from batteries. Figure 3 is a photograph of a PMIC that is used by iPhone 8. Such electronic devices often contain several sub-circuits, each with its own voltage level requirement different from that supplied by the battery or an external supply (sometimes higher or lower than the supply voltage). Additionally, the battery voltage declines as its stored energy is drained. A PMIC regulates the supply voltage to various loads such that the various circuits (sub-systems) provide the same performance even when the battery is not fully charged.

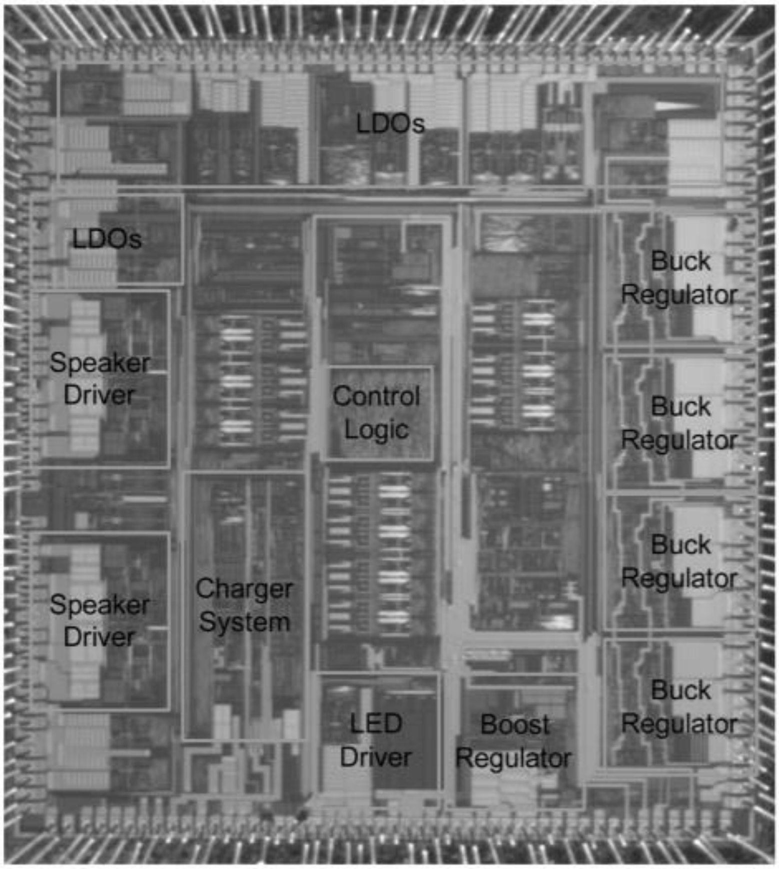


Figure 1: Die Photo of a PMIC for Mobile Applications [3]

For instance, Power-management ICs (PMICs) for high-voltage automotive applications are typically attached to the lead-acid battery (see Figure 2 for a depiction). This battery operates in the 9V to 16V range but has transient conditions that can go as low as 4V and as high as 40V. As such, they should be able to handle high input voltages as well as load dump events through the vehicle's lifetime. An automotive processor in standby mode, consuming a fraction of its peak power, will draw its full current when called to action. When this occurs, the switch-mode power supply's output voltage will dip temporarily, bouncing around before settling in at its target voltage. A well-designed power supply can manage the output voltage swing to prevent it from going out of spec and from hampering the processor's performance [8]. This is one of the desired functionalities of a PMIC.

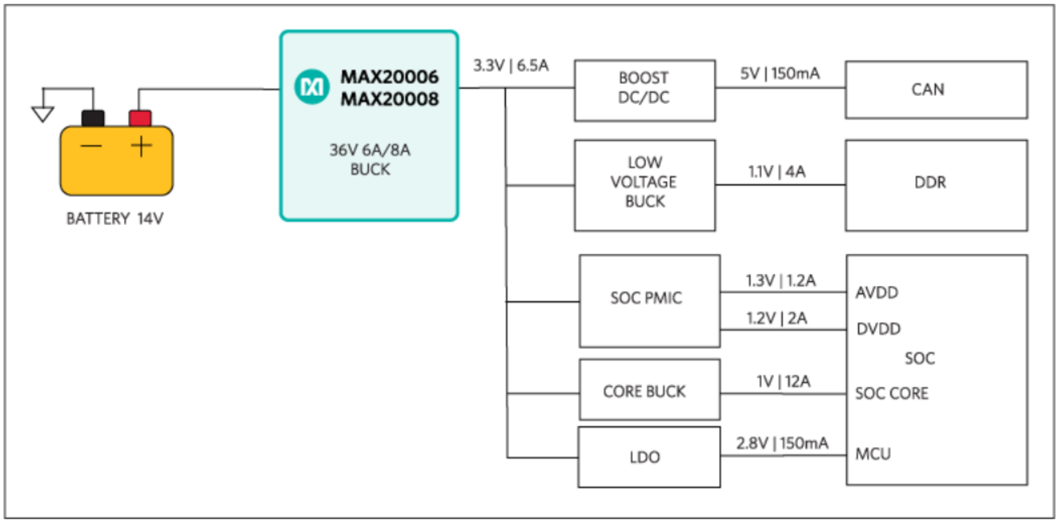


Figure 2: A Power Supply for Automotive Processors [8]

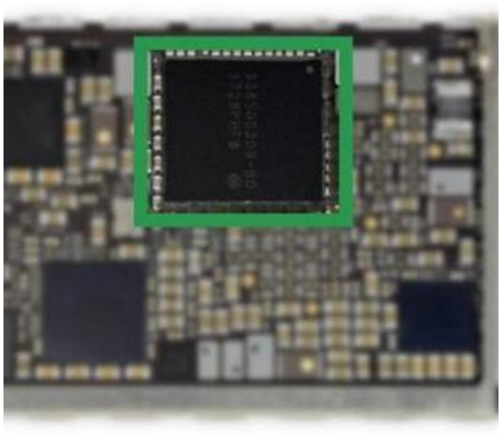


Figure 3: IPhone 8 and 8 Plus Big Main Power Management Chip PMIC (Image source: Google)

Apart from a regulated supply voltage they can provide power controls such as voltage supervision, undervoltage protection, etc. They can also carry out functions like reducing the supply voltage and clock frequency based on workload, also known as Voltage scaling. It can control the timing and sequencing of bias voltages which is termed as Power sequencing. Failure to follow the correct sequence could cause improper operation or excessive current flow caused by latch-up, or even catastrophic failure of the device under test (DUT). Figure 4 represents some of the functions carried out by PMICs.

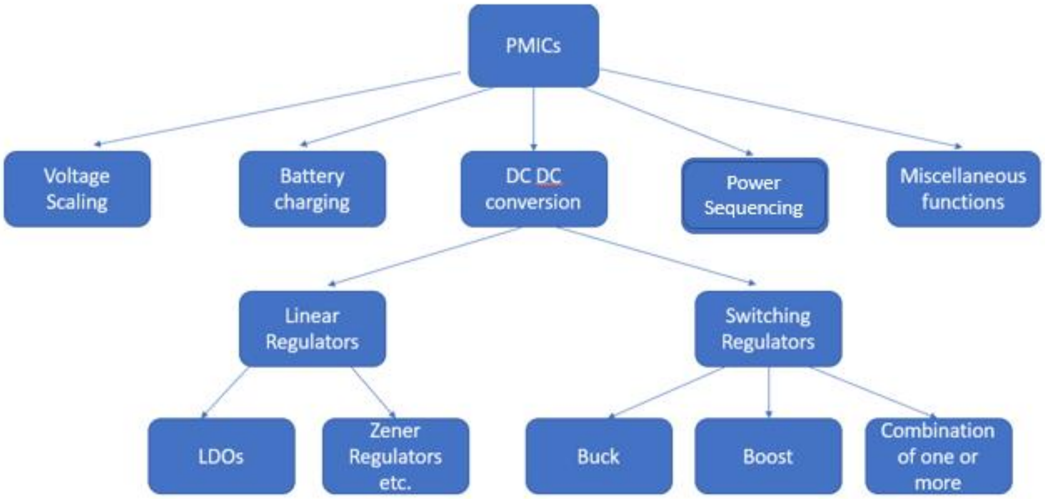


Figure 4: Brief Summary of PMIC Functions and Types

1.2 Background on Power Converter Architectures

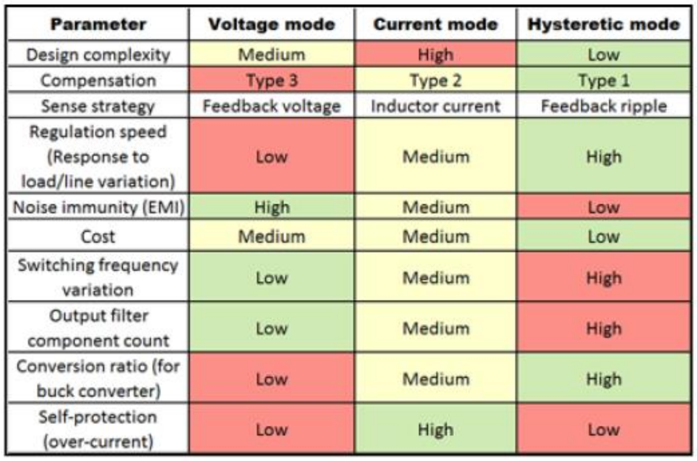
A major function of PMIC is DC-DC conversion, which is carried out by power converters. PMICs typically consists of multiple power converters. Power converters can be broadly categorized into 1) DC-DC switching regulators and, 2) linear regulators. A common type of linear regulator is the low-dropout regulator (LDO), which has the advantages of providing a low-noise regulated output with a relatively small size footprint and fast settling time. Unfortunately, these advantages come at the expense of reduced efficiency and limited applications because they can only provide a regulated output voltage that is lower than the input voltage.

On the other hand, DC-DC switching converters provide high-efficiency operation at the expense of larger physical footprint and noisy output. Switching converters can produce output greater than or less than the input voltage. Figure 5 summarizes the categories and their typical features.

	Buck	Boost	LDO	Multiphase buck
Operation type	Switching	Switching	Linear	Switching
Relative efficiency	High	High	Low	Medium High
Physical footprint	High	High	Low	Medium
Output ripple	High	High	Low	Medium
Load transient performance	Slow	Slow	Fast	Slow medium
Vout to Vin relation	Vout<Vin	Vout>Vin	Vout<Vin	Vout<Vin

Figure 5: Table Summarizing Types of Power Converters

LDOs are going to be preferred for small power requirements or when the input voltage is very close to the output voltage. They also tend to be physically smaller and less complex with fewer components. The inductor used in switching power supplies has a chance of producing audible noise. The increased efficiency is a major upper hand in switching supplies compared to LDO. Also, for LDO the output voltage will always be lower than the input voltage. But it’s a tradeoff between increased efficiency and lower noise, physical footprint area. In general, switching converters are used in battery-based, high load current applications and linear regulators are mostly used to power noise-sensitive analog and radio frequency (RF) circuits such as clock generators, envelope trackers, etc. For each of these DC-DC switching converters (Buck, Boost, etc.) there are a number of control techniques, based on the performance requirements of the converter. Commonly used control techniques are summarized in Figure 6.



Parameter	Voltage mode	Current mode	Hysteretic mode
Design complexity	Medium	High	Low
Compensation	Type 3	Type 2	Type 1
Sense strategy	Feedback voltage	Inductor current	Feedback ripple
Regulation speed (Response to load/line variation)	Low	Medium	High
Noise immunity (EMI)	High	Medium	Low
Cost	Medium	Medium	Low
Switching frequency variation	Low	Medium	High
Output filter component count	Low	Medium	High
Conversion ratio (for buck converter)	Low	Medium	High
Self-protection (over-current)	Low	High	Low

Figure 6: Table Summarizing Types of Control Techniques for DC-DC Switching Converters

- Voltage mode control: Where the output voltage of the converter is sensed and compared against a reference and processed to generate a signal of a certain duty cycle, which further adjusts the output voltage.
- Current mode control: Where the inductor current is sensed,
    a. Peak current mode control: Instead of driving it by sensing the output voltage to generate a duty cycle, the inductor current is sensed against a peak value to switch the transistor off when the peak value is reached.
    b. Average current mode control: In addition to sensing the inductor current, the output voltage is also sensed to generate the reference for the current sensing loop.
- Hysteric mode control: It performs controls by detecting ripples in the output, this method is also referred to as a ripple control method. The method directly monitors the output voltage by means of a comparator without going through an error amp. When detecting that the output voltage has exceeded or fallen below a set threshold level, the comparator directly turns the switch on/off.

Each control technique has its own advantages/disadvantages and is used based on the application. Advantages of voltage mode control method are its relative simplicity based on the use of a feedback loop consisting solely of voltages, the ability to control shorter on-time, and high noise tolerance. However, the design of the phase compensation circuit is cumbersome. On the other hand, the current control mode has a simplified phase compensation circuit design. The average controlled current mode has some advantages over Peak current controlled mode, it has better noise immunity, can control average current accurately in a wide range of applications. But unlike Peak current mode, it does not have built in protection against overcurrent failure. Average current controlled mode has two feedback loops unlike Peak current controlled mode. One for sensing the inductor current and comparing it to a reference, whereas the second loop is used to generate the reference by sensing the output voltage, which makes the circuit analysis relatively complicated. Hysteric control mode has the advantage of extremely fast transient responses due to the direct control exerted by a comparator and the elimination of the need for phase compensation. The method suffers from the problems of variable switching frequencies, large jitter, and the need for an output capacitor with a relatively large equivalent series resistor (ESR) for output ripple detection.

1.3 Motivation for Monitoring Power Management Circuits

Current typical power management circuits don’t have the adaptability to the changing environment of the circuit. Complex electronic systems deal with drastically varying power environment. Switching converters with high frequency of operation have been gaining importance in the market due to their compactness in size and high efficiency. But as the switching frequency increases and the filter components become smaller in size, their variability across process variations increases. It might degrade to an extent that renders the system operation unstable.

Almost all voltage regulators need a feedback loop to maintain a constant regulated output voltage. As with any feedback loop, there is some phase shift associated with the loop and that determines the loop stability. To have a stable system the phase shift across the loop should be less than 180 degrees at the point where the loop has unity gain or 0 dB gain to keep it from oscillating or going unstable. Compensation circuits with various passive components are utilized to maintain a decent phase margin across process corners, this is employed in both linear as well as switching converters. Switching converters also use an output filter to reduce the noise from switching. But the variation in these passive components can lead to degraded performance (lower efficiency, increased noise, lower disturbance rejection, etc.), instability and even failure of the system.

The component (inductors, capacitors, switching MOSFETs) variations either in the power stage or input filter of the DC-DC converter can degrade the performance, cause instability leading to probable failure of the system. The variation in their value while operating must be considered, typical inductors and capacitors have a nominal variation of +/- 10% in value. The aging of the capacitors should also be considered. This aging causes a significant change in the value of the capacitance and the external series resistance (ESR). Typical variations due to aging are of on the order of 30% for capacitance [4], up to 200 % for ESR [5]. Temperature dependence of inductance and capacitance also cause variations. An overall variation of 20% in inductance, 50% in capacitance and 200% in ESR is possible [6]. Figure 7 shows the efficiency degradation over the lifetime of power converters in different applications. This research investigates methods for monitoring these changes.

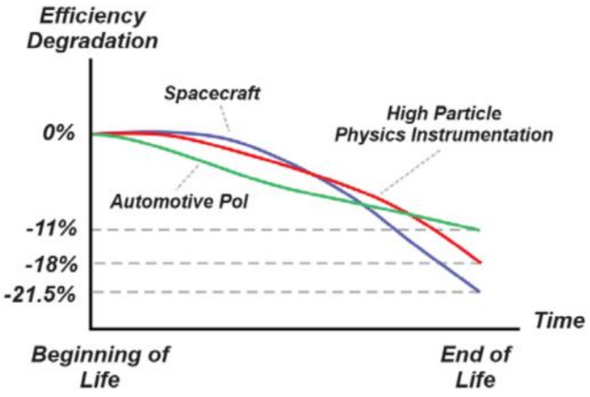
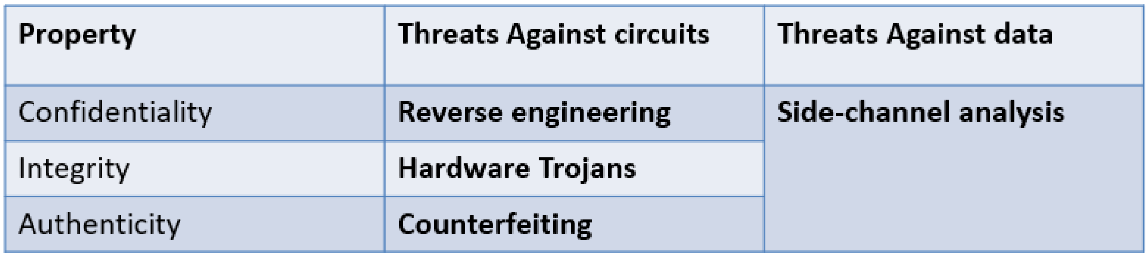


Figure 7: Efficiency Degradation in Power Converters Due to Aging in Different Applications

Apart from performance, security and reliability are also concerns. Designing an IC involves procuring intellectual property (IP) designs from third-party design houses, simulating it for specifications and then generating a layout of the circuit. A blueprint of the design is sent to the foundry that is supposed to manufacture the IC. The ICs are then tested at the manufacturing site and often also at third-party test facilities. Finally, once the silicon die is back from the foundry, the ICs are packaged and sold [12]. There are multiple points within this supply chain that pose an opportunity to inject malicious hardware into the IC. There are numerous types of hardware threats including,

- Hardware Trojans: An attacker may add malicious circuits or modify existing circuits which might alter the existing functionality of the circuit.
- IP piracy and IC overbuilding: An IP user or a rogue foundry may illegally pirate the IP without the knowledge and consent of the designer. A malicious foundry may build more than the required number of ICs and sell the excess ICs in the gray market.
- Reverse engineering (RE): An attacker can reverse engineer the IC/IP design to his/her desired abstraction level. He can then reuse the recovered IP or improve it.
- Side-channel analysis: An attacker can extract the secret information by exploiting a physical modality (power consumption, timing, or electromagnetic emission) of the hardware that executes the target application.
- Counterfeiting: An attacker illegally forges or imitates the original component/design [12].



Property	**Threats Against circuits**	**Threats Against data**
Confidentiality	**Reverse engineering**	**Side-channel analysis**
Integrity	**Hardware Trojans**	
Authenticity	**Counterfeiting**	

Figure 8: Classification of Security Attacks

A hardware Trojan is an unexpected/malicious modification to a circuit. The Trojan may control, modify, disable, or monitor the contents and communications of the underlying computing device [14]– [16]. A Hardware Trojan may be able to defeat all security mechanisms (software or hardware-based) and subvert or augment the normal operation of an infected device. This may result in modifications to the functionality or specification of the hardware and the leaking of sensitive information [18]. Since hardware trojans may be activated in the field after deployment, it may or may not be detected by post-production testing. But these can be detected by an online Built-in self-test circuit that monitors the system for altered functionality.

1.4 Background of BIST

Built-in self-test is a mechanism that permits a machine to test itself. The main purpose of BIST is to reduce the complexity, and thereby decrease the cost and reduce reliance upon external (pattern-programmed) test equipment. Several methods have been proposed to self-test DC-DC converters using various test signals, to characterize the converters. Some techniques require the converter to be in open-loop and thus cannot reliably supply the connected load during testing, while others can be used in closed-loop, but are only applicable to digitally controlled systems. Many of these techniques have high hardware and computational requirements.

It is usually not enough to monitor and qualify the system only during the manufacturing process as system performance and circuits can also be affected at the customers end during field operation. So, a method is needed that can monitor the system while it's operating without disturbing the normal mode of operation. It should typically have the following properties,

1. The system identification technique should have minimal effect on the output voltage of the converter.
2. Loop measurements need to be conducted during closed loop operation, at the operating point of the system.
3. System output response should have enough dynamic range.
4. The measurement needs to present little to no computational overhead and silicon die area.

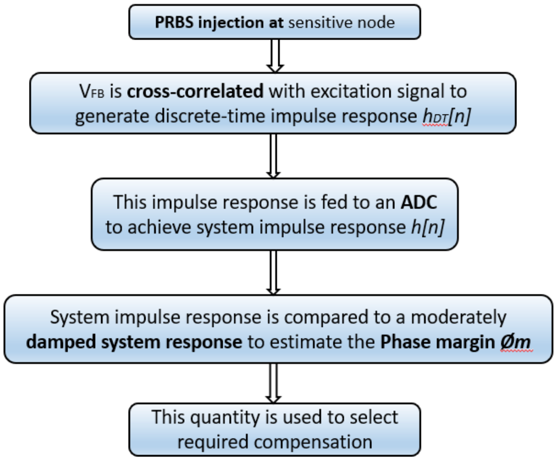

PRBS injection at sensitive node
V_{FB} is **cross-correlated** with excitation signal to generate discrete-time impulse response $h_{DT}[n]$
This impulse response is fed to an **ADC** to achieve system impulse response $h[n]$
System impulse response is compared to a moderately **damped system response** to estimate the **Phase margin** $Ø_m$
This quantity is used to select required compensation

Figure 9: Flow Chart Representing Steps for PRBS Injection to Determine Phase Margin

Figure 9 summarizes the steps to determine the phase margin using PRBS injection. To reduce the complexity of processing the signals obtained from the system identification process, instead of first sampling the output voltage using a high-bandwidth, high-accuracy ADC and then cross-correlating, the signal will be cross-correlated first and then sampled [19]. This relaxes the specification of the required ADC. To aid in relaxing the ADC specifications, analog correlator is used which has low storage and computational requirements. Processing the correlation in the analog domain using an analog correlator instead of the digital domain, results in less ADCs than required in digitally controlled DC-DC converters.

While the DC-DC converter is highly non-linear, in steady state, for small disturbances around the operating point, the system can be modeled as a linear, time-invariant system. The transfer function of such a system can be obtained in many ways:

(a) applying a sinusoidal waveform, measuring gain and phase, and sweeping the frequency to characterize the system,

(b) applying a step function, measuring the time domain response and fitting the response to a known structure of the transfer function,

(c) applying a wide bandwidth signal, and taking the spectrum of the output, which would correspond to the transfer function of the system if the input is wide-band enough.

Out of these techniques (a) is not feasible because it generates tones at the output which may make other components unstable, and (b) is not feasible because for a step input small enough not to disturb the normal operation mode, the target measurements (in the form of ripple, overshoot, undershoot) are not feasible. To enable option (c), a wide-bandwidth signal needs to be generated to excite the converter and monitor the response in the background.

Additionally, the technique should not interfere with the proper operation of the load being supplied nor should it have EMI concerns. Hence, the test signal used should be such that the test signal energy is spread across the frequency spectrum and should not be concentrated at one (or more) frequencies. Hence, PRBS is used as the test signal of choice as against using frequency-swept sinusoidal methods.

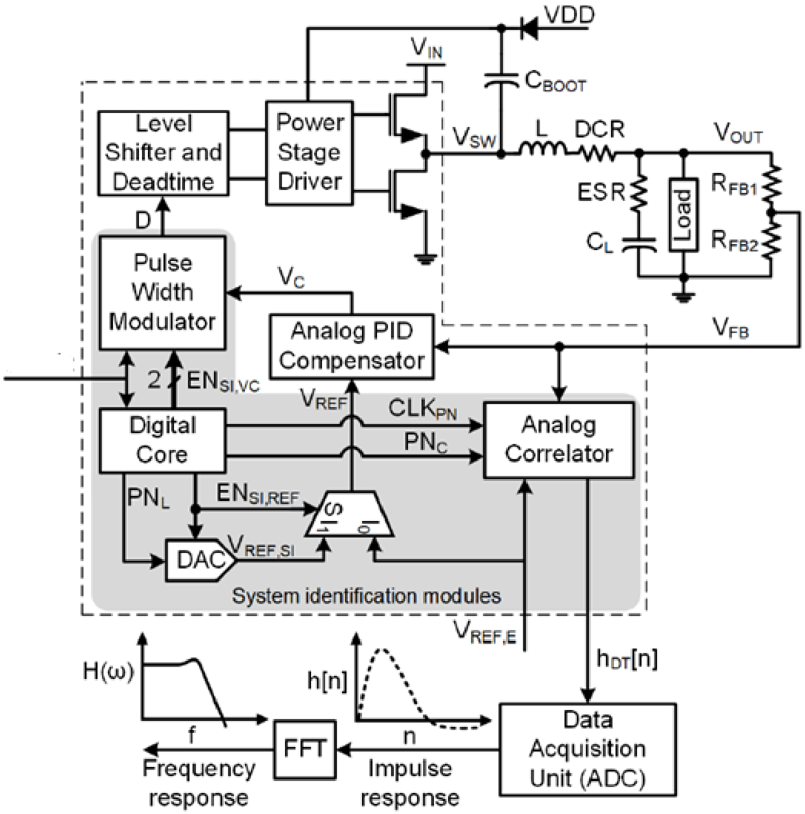


Figure 10: System Level Architecture of the DC-DC Buck Converter IC with Integrated System Identification Modules [19]

Due to the complexity of generating complex test signals on-chip, a simple stimulus which can be generated without complex implementation would be the most suitable for IC implementation. Thus, a single bit PRBS is used among other available options such as multi-bit or multi-level PRBS. To inspect the operation of the DC-DC converter, the changes in the dynamic loop characteristics of the DC-DC converters needs to be tracked without disturbing the normal mode of operation.

1.5 Correlation Based Dynamic Loop Characterization - Motivation Behind Injecting Pseudo Random Binary Sequence (PRBS) Signal

In steady state operation, for small signal disturbances, a switching power converter can be approximated as a linear time-invariant discrete-time system [1]. A linear time-invariant sampled system can be described as,

$$y[n] = \sum h[k].x[n-k] + v[n]$$

Where y[n] is the sampled output signal, x[n] is the sampled input signal, h[n] is the discrete-time system impulse response and v[n] represents unwanted disturbances, such as switching noise, quantization noise, etc. The cross-correlation of the input signal x[n] and the output signal y[n] is as follows:

$$R_{xy}[m] = \sum x[n].\, y[n+m]$$

$$R_{xy}[m] = \sum h[n].\, R_{xx}[m-n] + R_{xv}[m] \qquad (1)$$

Where Rxy[m] is the cross-correlation of the input and output signals, Rxx[m] is the auto-correlation of the input signal and Rxv[m] is the cross-correlation of input signal with disturbances [10]. Now, if x[n] is white noise, then correlation functions R_{xx} and R_{xv} have the following properties,

$$R_{xx}[m] = \delta[m]$$
$$R_{xv}[m] = 0$$

Where δ[m] is an ideal delta function. Auto-correlation of white-noise input is ideal delta function and cross-correlation of white-noise input with unwanted disturbances v[n] is ideally zero. This simplifies Eq. (1) and the cross-correlation becomes the discrete-time system impulse response [10].

The properties presented above need the injection signal to be white noise. In addition, it is desirable that the signal generation adds low overhead. In practical implementation, an approximate white noise is generated by pseudo random binary sequence (PRBS) generator consisting of shift registers and feedback taps [11]. The PRBS noise is injected at different points in the loop and correlation is done at the output. BIST circuit measures the impulse response in the time domain. Stability parameters, such as phase margin, can be calculated based on the impulse response.

Previous work represents a technique to track changes in the dynamic loop characteristics of the DC-DC switching converters controlled by sensing the output voltage (voltage mode control) without disturbing the normal mode of operation using a white noise-based excitation and correlation [1].

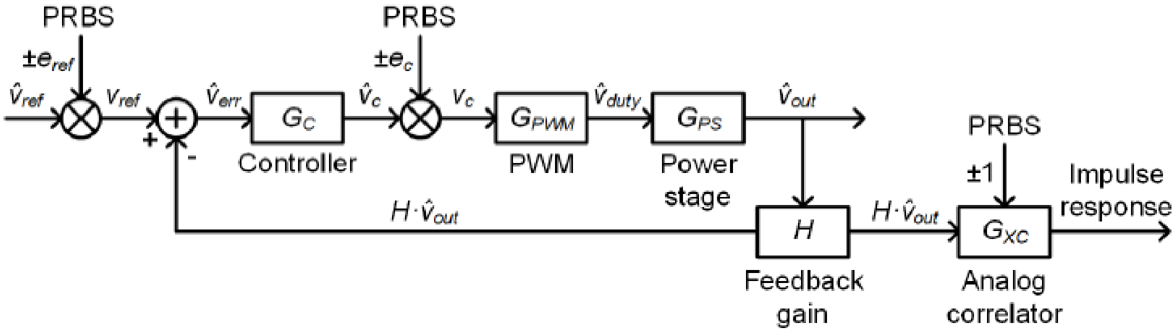


Figure 11: AC Small- Signal Model of the Proposed Converter Loop with Online Built-In Self-Test [19]

The PRBS signal was injected at two points in the loop, due to different forward TF for injection at both these points it lets us localize the source of change.

The average current control mode has two loops unlike voltage or peak current control mode, that gives us a multitude of points to inject the PRBS signal. The following chapter discusses the injection points for the PRBS so that it can track the changes detecting if the system is operational with satisfactory performance.

CHAPTER 2

INJECTION POINT ANALYSIS FOR BUCK CONVERTER IN AVERAGE CURRENT MODE CONTROL

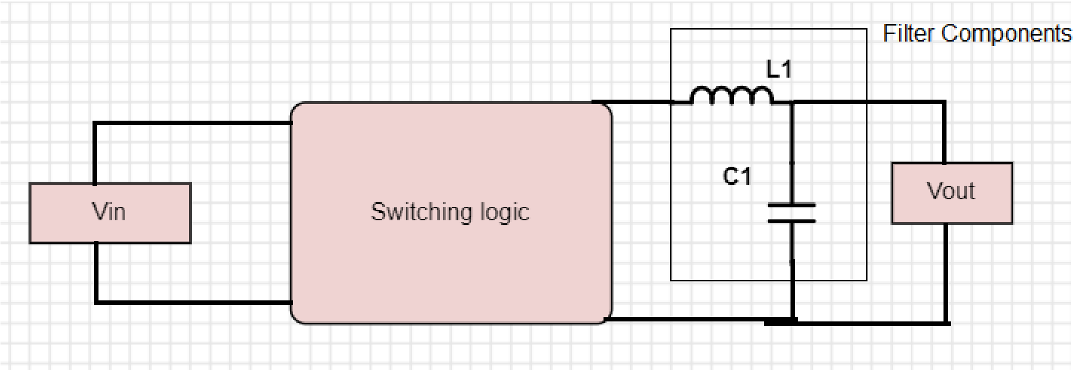


Figure 12: Typical Buck Converter

A Buck converter steps down voltage (while stepping up current) from its input (supply) to its output (load). The amount by which it is stepped down is determined by the duty cycle of the switching signal. L1 and C1 form a low pass filter to reduce voltage ripple. Figure 12 shows a typical buck converter. The switching logic is realized by typically at least two semiconductors (a diode and a transistor, although modern buck converters frequently replace the diode with a second transistor used for synchronous rectification).

2.1 Average Current Mode Control

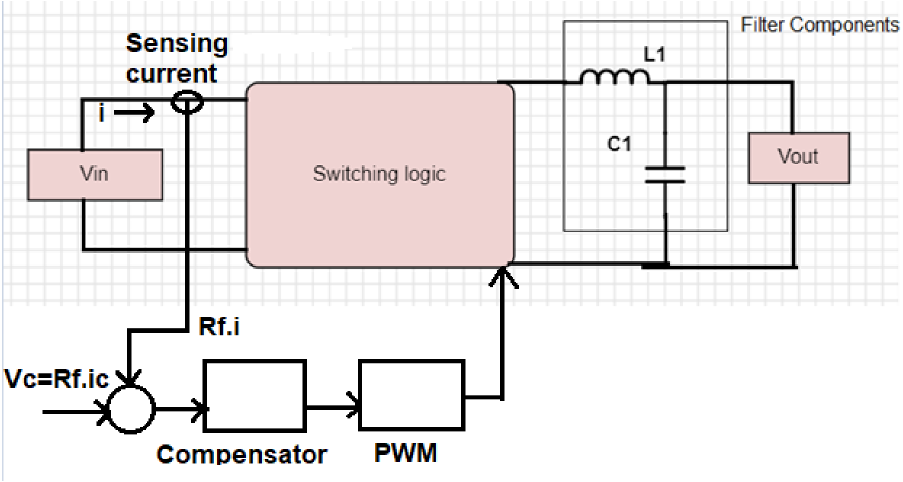


Figure 13: Buck Converter with Current Sensing Loop

Figure 13 shows a Buck converter in Average current control mode. Here, the inductor current is sensed with an equivalent current sensing resistor Rf, the sensed signal is compared to a reference or control input Vc, the error between the two is processed by a current loop compensator. The output of the compensator is applied to a Pulse width modulator which generates a control signal for the switching logic.

The reason it is called Average mode control is that in the process of comparing and processing the error signal between the sensed current and reference current, a compensator is employed which typically has a low pass nature, that filters out high-frequency components and ripples in the sensed current. In effect what is really controlled in the loop is the average value of the sensed signal, and that’s where the name comes from.

To control the output voltage, an additional outer voltage loop is closed, which generates the reference signal for the inner current loop.

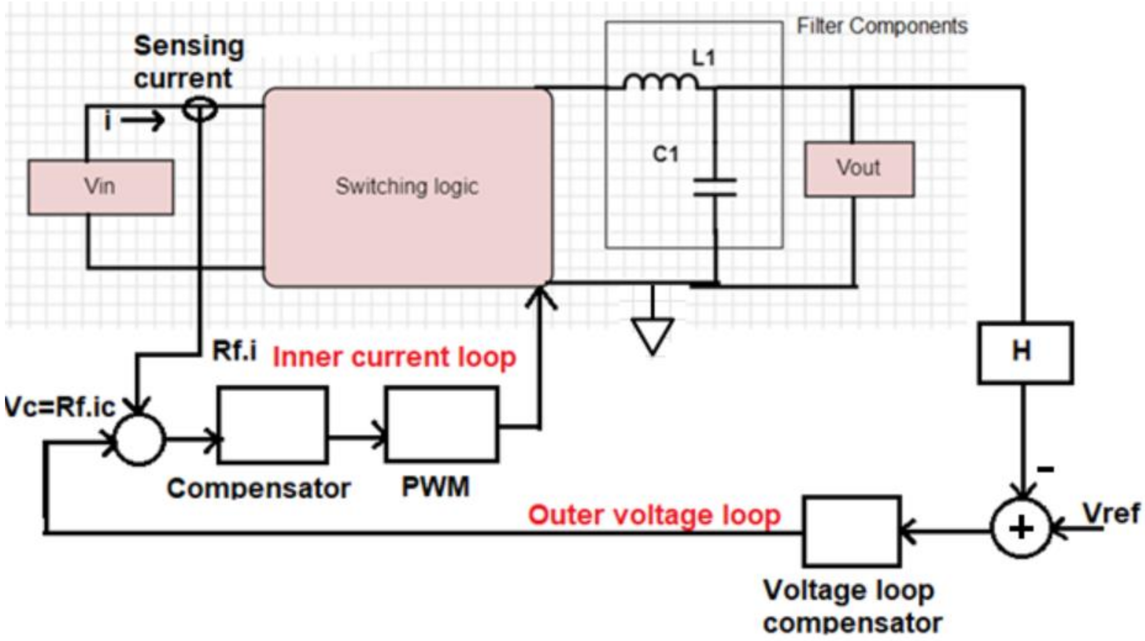


Figure 14: Buck Converter in ACM Mode, Showing Both the Control Loops

The output voltage is compared with a reference to generate an error signal, which is processed by the compensator to generate the reference for the inner current loop.

In average current controlled mode, two loops must be stabilized, let’s analyze the injection points which will help isolate the cause for instability. Section 2.2 analyses any general system with control loops.

2.2 Multiple Loop System with Inner and Outer Loops

As the average current mode control has two loops, the stability criteria of a general system with two control loops will be analyzed in this section by breaking the loop (injecting noise) at different points. Figure 15 shows any typical system with multiple control loops, whereas A and B are the forward gains. Y is the output signal and X is the input, 1 and 2 are the points where the loops will be broken to estimate loop gains. H1 and H2 the feedback factor each of the loops.

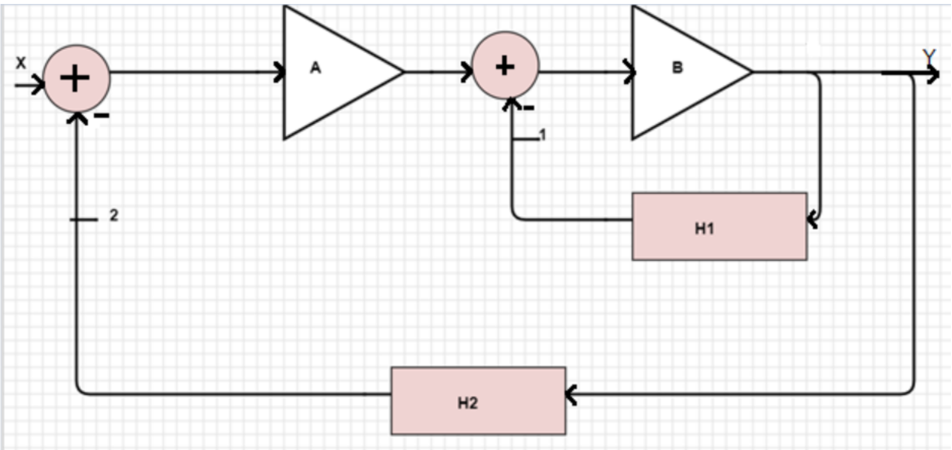


Figure 15: Any General System with Multiple Control Loops

Total response of the closed loop system can be derived as:

$$\frac{Y}{X} = \frac{A.B}{(1 + H1.B + H2.A.B)}$$

Loop gain when loop is broken at 1:

$$\frac{B}{1 + H2.A.B}$$

Loop gain when loop is broken at 2:

$$\frac{A.B}{1 + H1.B}$$

From the total response of the system, it can be seen that for the system to be stable, (H1.B+H2.A.B)≠-1 needs to be ensured, individual stability (H1.B≠-1 or H1.A.B≠-1) is not required, the addition should be stable.

Similarly, for current and voltage loops, it can be designed as one to be the stable loop another to be the faster (high bandwidth) loop. Ensuring that both are stable individually by a high phase margin is not required.

2.3 Design of the Current and Voltage Loops

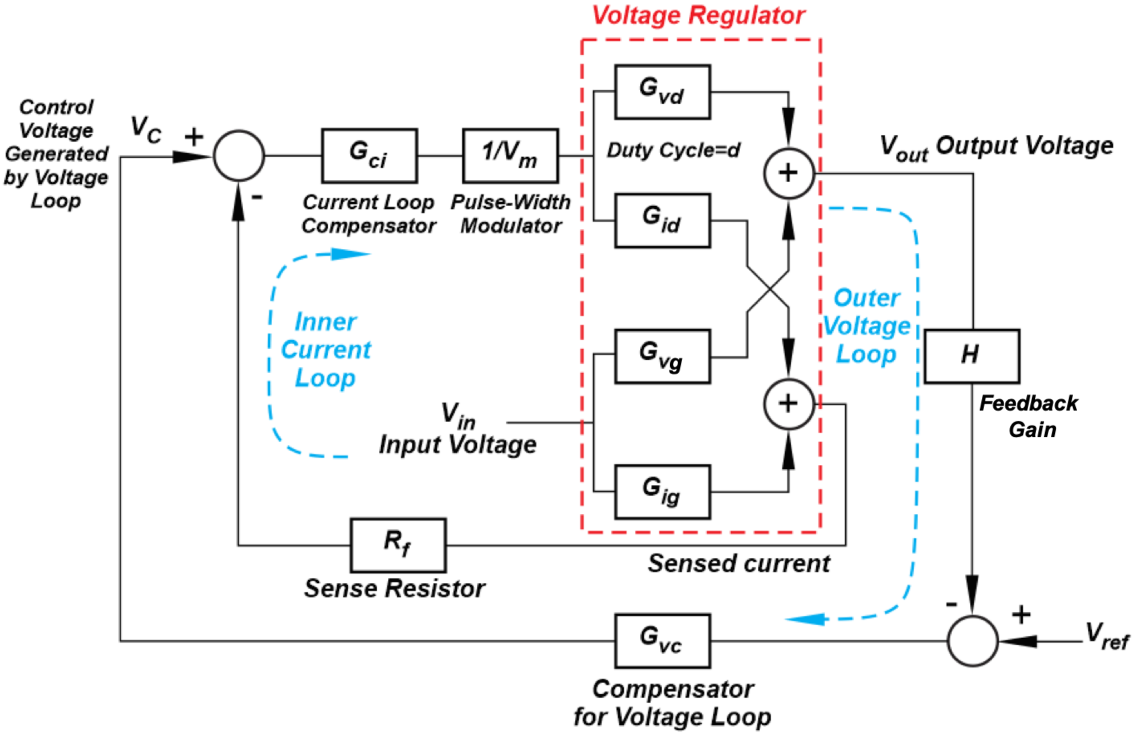


Figure 16: Both the Control Loops in an ACM Buck Converter with all the Transfer Functions

In figure 16, the duty cycle (d) to output voltage is described by the transfer function G_{vd}, duty cycle to sensed current transfer function by G_{id}. Similarly, input voltage to output voltage and input voltage to sensed current transfer functions are defined by G_{vg} and G_{ig} respectively. V_C=R_f.i, is the reference generated by the outer voltage loop by sensing the output voltage loop. Compensator for the current sense loop (G_{ci}) is designed for a desired phase margin and crossover frequency, after observing the response without the compensator, same goes for the compensator for the voltage loop (G_{cv}). Transient response time depends on the crossover frequency of the response. Ringing and overshoot in the response depends on the phase margin of the response.

2.3.1 Closed Loop Transfer Function for the Injection Points

To diagnose the changes in the system dynamics of the converter, PWM node, the current loop reference node and the voltage loop reference node, are chosen as the stimulus points and the output voltage node is chosen as the observation point for the respective loops. From figure 12,

1. PWM input node disturbance rejection transfer function is given by:

$$\frac{Gid.(\frac{1}{Vm})}{1+Gid.Gci.\left(\frac{1}{Vm}\right)Rf}$$

Loop gain of the current loop shown in Figure 16 can be derived as (T_i):

$$T_i = R_f.G_{ci}.\frac{1}{V_m}.G_{id} \qquad (1)$$

2. Closed loop current loop reference (V_C) to sensed current (i) transfer function:

$$\frac{i}{V_C} = \frac{T_i}{R_f(1+T_i)} \qquad (2)$$

$$=> \frac{Gci.Gid.(\frac{1}{Vm})}{1+Gid.Gci.\left(\frac{1}{Vm}\right)Rf}$$

3. Closed loop voltage loop reference (Vref) to output voltage transfer function:

First, formulating a relation between the voltage and current loops to simplify the analysis. From figure 16, simplifying the part from V_C to V_{out}, including the inner current loop.

As the Voltage loop is the slower loop and has a smaller crossover frequency than the faster current loop, so at the crossover frequency of the voltage loop i.e. at frequencies well below the crossover frequency of the current loop (T_i>>1), (2) can be written as:

$$\frac{i}{V_C} = \frac{1}{R_f}$$

This simplification of $\frac{i}{V_C}$ transfer function forms the basis for design of the voltage loop.

For the current loop, the inductor current(i) is sensed to produce duty cycle (d) and the transfer function of the current loop is given by:

$$G_{id} = \frac{i}{d}$$

Combining $G_{id} = \frac{i}{d}$ and $\frac{i}{V_C} = \frac{1}{R_f}$

$$=> \qquad i = \frac{V_C}{R_f} = G_{id}.d$$

$$=> \quad \frac{d}{V_C} = \frac{1}{G_{id}.R_f} \qquad (3)$$

Similarly, for the voltage loop output voltage (V_{out}) has been sensed to produce the control voltage (V_C) and the transfer function of the voltage loop is given by:

$$G_{vc} = \frac{V_{out}}{V_C}$$

multiplying numerator and denominator with duty cycle(d),

$$= \frac{V_{out}.d}{d.V_C} \qquad (4))$$

The following equations will be mathematically modified to simplify the voltage loop transfer function: $G_{vc} = \frac{V_{out}}{V_C}$.

The transfer function of duty cycle to output voltage can be written as, $G_{vd} = \frac{V_{out}}{d}$ and using this in equation (4):

$$G_{vc} = \frac{G_{vd}.d}{V_C}$$

and from equation (3) $\frac{d}{V_C} = \frac{1}{G_{id}.R_f}$, using this in G_{vc} equation above:

$$G_{vc} = \frac{V_{out}}{V_C} = \frac{G_{vd}}{G_{id}.R_f}$$

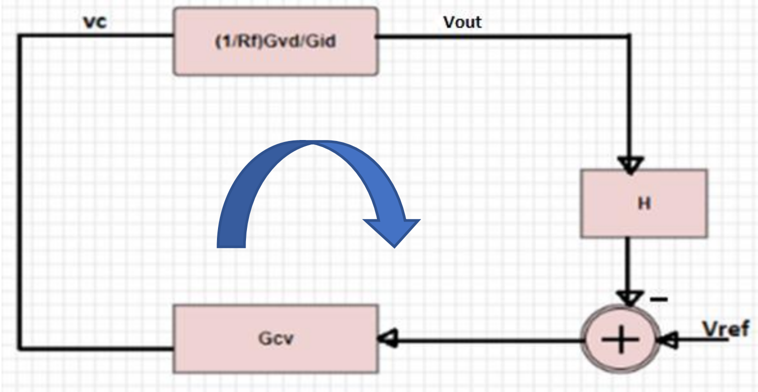


Figure 17: Outer Voltage Loop of Converter in Average Current Control mode

So, the voltage loop can be simplified as shown in Figure 17, this is the estimated transfer function of V_C to output voltage (V_{out}), Due to the simplification above, loop gain of the voltage loop can be written as,

$$T_v = \left(\frac{1}{R_f}\right).\left(\frac{G_{vd}}{G_{id}}\right).H.G_{vc} \quad (6)$$

Finally, the closed loop reference-to-output transfer function is given by,

$$\frac{V_{out}}{Vref} = \frac{T_v}{H.(1+T_v)} => \frac{\left(\frac{1}{Rf}\right).\left(\frac{Gvd}{Gid}\right).Gcv}{\left(1+\left(\frac{1}{Rf}\right).\left(\frac{Gvd}{Gid}\right).H.Gcv\right)} \qquad (7)$$

2.3.2 Estimation of Gvd and Gid Using Small Signal Model:

The transfer functions used section 2.3.1 will be derived in this subsection to understand the dependence of these on passive components used in the converter. Where the duty cycle (d) to output voltage is described by the transfer function G_{vd}, duty cycle to sensed current transfer function by G_{id} as depicted in figure 16.

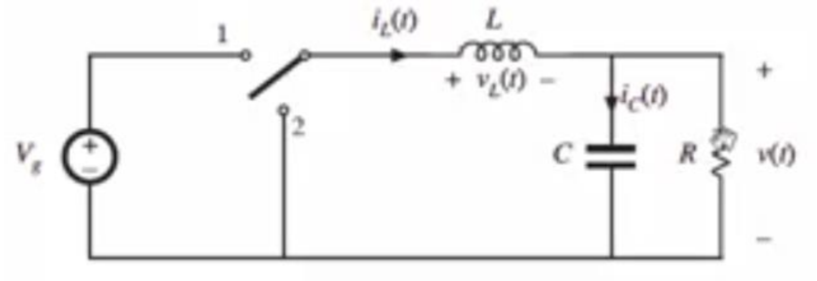


Figure 18: Simplified Diagram of a Single-Phase Buck Converter

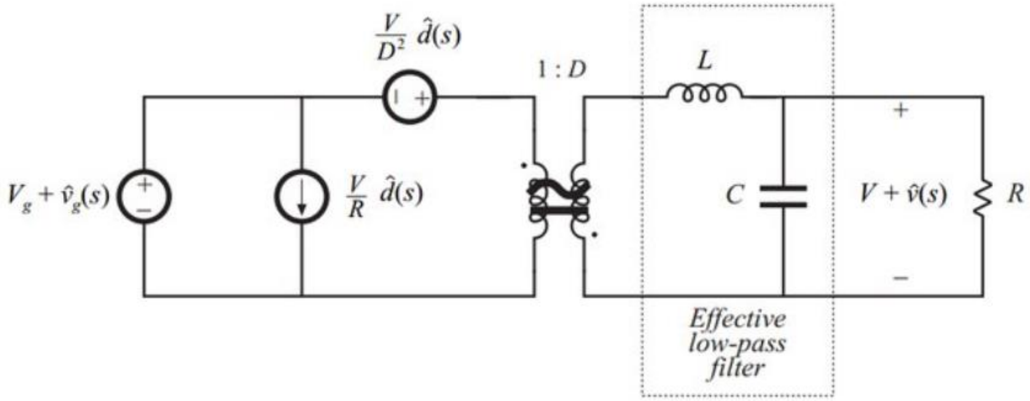

$\frac{V}{D^2}\,\hat{d}(s)$
1 : D
L
+
$V_g + \hat{v}_g(s)$
$\frac{V}{R}\,\hat{d}(s)$
C
$V + \hat{v}(s)$
R
−
Effective low-pass filter

Figure 19: Small Signal AC Model of the Buck Converter [9]

Gid estimation using the small signal model of the Buck converter [1]:

$$Gid = \frac{i}{d} = \frac{Vg(1 + sCR)}{R\left(1 + s^2LC + s.\frac{L}{R}\right)}$$

Gvd estimation using the small signal model of the Buck converter [1]:

$$Gvd = \frac{v}{d} = \frac{Vg}{\left(1 + s^2LC + s.\frac{L}{R}\right)}$$

Putting the derived Gid and Gvd values in the closed loop reference-to-output transfer function (7),

$$\frac{R}{Rf(1 + sCR) + H.R} \quad (8)$$

This is a first order equation as opposed to the second order response in Voltage mode control [2].

2.4 PRBS Injection Points

The following summarizes the injection points for monitoring the system based on the derivations above:

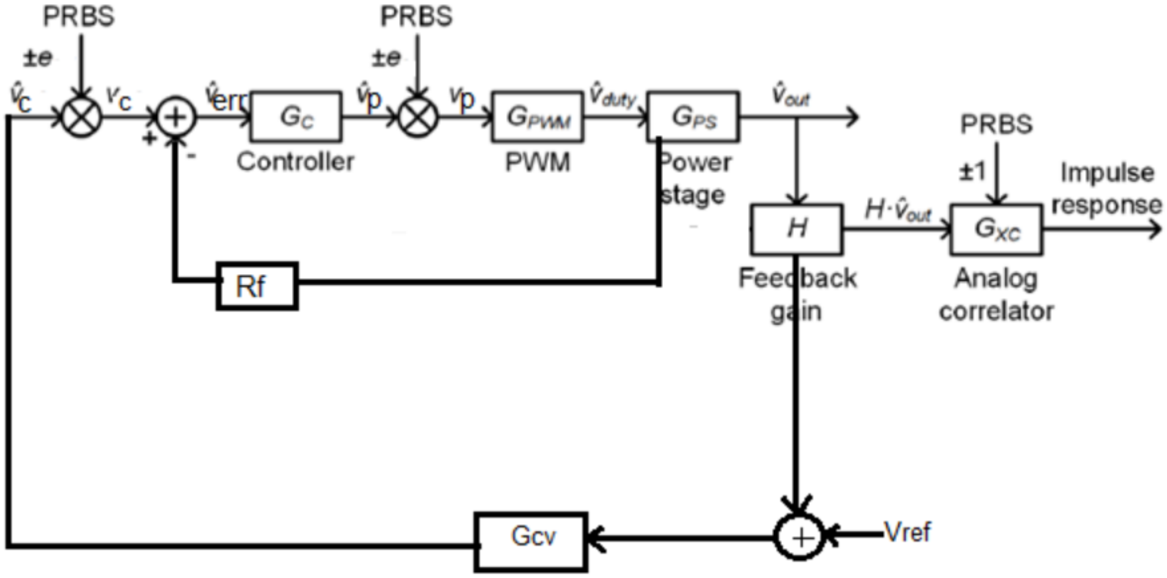


Figure 20: AC Small-Signal Model of the Proposed Converter Loop with Online Built-In Self-Test.

- The PRBS is injected at multiple points to let us characterize different transfer functions (TF).
- Even if the loop TF is same in both cases, due to different forward TF in the path it localizes the source of change. So, in case one TF has changed significantly with respect to the ideal expected TF for that path, that part of the loop can be pointed.

- If in addition to Vout, cross-correlation can also be performed at input of PWM node, then that will decouple all the major building blocks in the loop block diagram and will help localize the source of change more accurately.
- High impedance (like gate of a transistor) for injection is suitable for injection so that the operating point of the loop is not changed.
- Previous work, for Voltage Mode Controlled Buck converter injection points were Vref and input of PWM [2].
- The possible injection points are Vc, Vref and input of the PWM from figure 16.
- In Average Current Control Mode, derived previously,
- Closed loop transfer function for injection at Vref (from (7)):

$$\frac{Gcv.(\frac{1}{Rf})(\frac{Gvd}{Gid})}{1+Gcv.(\frac{1}{Rf})(\frac{Gvd}{Gid}).\mathrm{H}}$$

- Closed loop transfer function for injection at PWM input:

$$\frac{Gid.(\frac{1}{Vm})}{1+Gid.Gci.\left(\frac{1}{Vm}\right)Rf}$$

- Closed loop transfer function for injection at Vc:

$$\frac{Gid.Gci.(\frac{1}{Vm})}{1+Gid.Gci.\left(\frac{1}{Vm}\right)Rf}$$

2.5 Conclusions

In previous work [19], for monitoring a Buck converter in Voltage mode control, PRBS was injected at Vref and PWM input. Average current control mode has multiple loops and relatively a greater number of points for injection are expected. A mathematical analysis of all the injections points is done to verify the type of response and expected results from it.

- Looking at the equations above, injection at Vref is not able to provide parameters like damping factor, Q, etc. as $\frac{Gvd}{Gid}$ cancels the second order equation that provides us with the information. (eqn.(8))
- Won't be able to derive the Phase margin using impulse response as well, there won't be peaking as the response is first order (due to the way the loops are designed).
- Hence, favorable injection points are Vc and PWM input.
- Two loops do not provide more points for injection compared to a single loop Voltage Mode Control. Therefore, the BIST is still limited to two points of injection at Vc and input of PWM.

CHAPTER 3

PERFORMANCE ANALYSIS OF LOW DROPOUT REGULATORS PRONE TO SECURITY ATTACKS

When it comes to powering noise-sensitive analog/RF applications (such as commonly found in test and measurement systems, where the measurement accuracy of the machine or equipment needs to be orders of magnitude better than the entity being measured), Low Dropout Regulators (LDO) are generally preferred over their switching counterparts. It is very common to use digital circuits to enhance the performance of an LDO. A malicious circuit inserted in a system typically affects the digital part of the circuit causing bit flips and so on, which gives a motivation to monitor these circuits while operating in the field. These malicious circuits don't affect the LDO to completely shut it down, which would be easily detectable but instead it hampers the performance of the LDO slowly and gradually, making them very difficult to detect.

3.1 Low Dropout Regulators

Power management is essential in all battery-powered portable devices. Low-dropout regulators are one of the most critical power management modules, as they can provide regulated low-noise and precision supply voltages for noise-sensitive analog blocks [20]. LDOs are a class of power converters that are relatively less noisy, smaller in size at the cost of lesser efficiency. The fundamental principle behind is to control the gate voltage of the pass transistor to maintain a constant voltage at the output node. The pass transistor can be NMOS or PMOS. The NMOS pass transistor LDO has an advantage of easier compensation to have a decent phase margin across all load conditions but typically needs a charge pump to drive the pass transistor. On the other hand, the PMOS pass transistor LDO is relatively difficult to compensate but doesn't require a

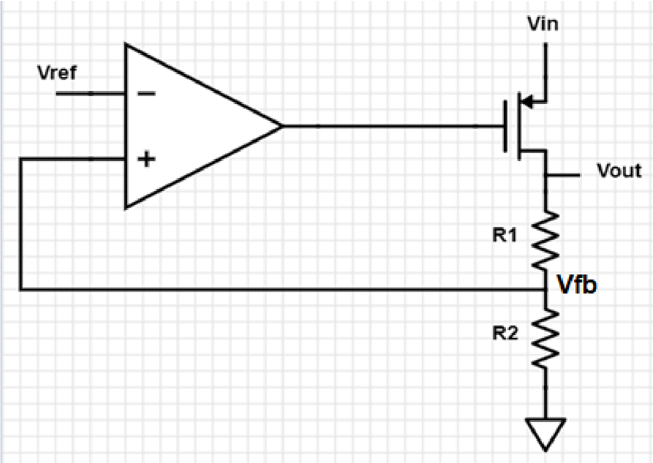


Figure 21: Basic Architecture of a Typical PMOS Passfet LDO

charge pump to drive the power transistor. LDOs are used when Vout is close to Vin, the minimum Vin – Vout required for stable operation on the LDO is known as the dropout voltage.

In figure 21, Vout can be made programmable by controlling the R1 and R2 values. Vfb is a fixed voltage, based on Vref which is usually supplied a Bandgap reference circuit. As it's a closed loop system, stability is a very important factor. To have a stable system there should be a sufficient phase margin. Low phase margin hampers the transient response by increasing settling times and on the other hand, very high phase margin causes slow response.

3.2 Design of the LDO

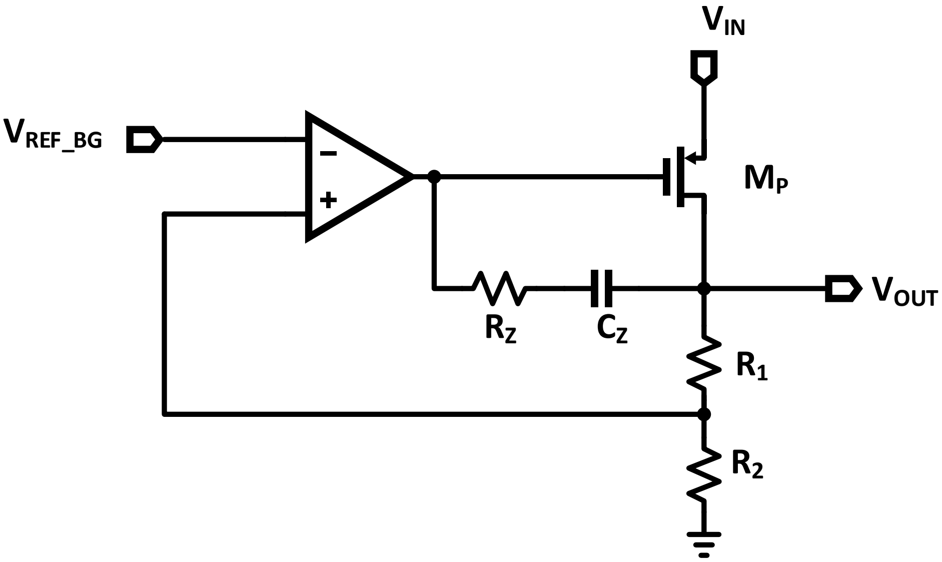


Figure 22: Designed LDO Architecture

Figure 22 shows an LDO with PMOS pass transistor has been designed with a nominal output voltage of 3.3V whereas nominal Vin value is 5V. It has a BGR providing a reference voltage of 1.2V and a capacitive load of 1uF. The operating load current range is 1nA to 30mA. A miller cap of 10pF and resistor of 500k Ω are used to stabilize the LDO across the load range. R_1 and R_2 denotes the resistor divider. The typical characteristics of the LDO are documented in section 3.2.1.

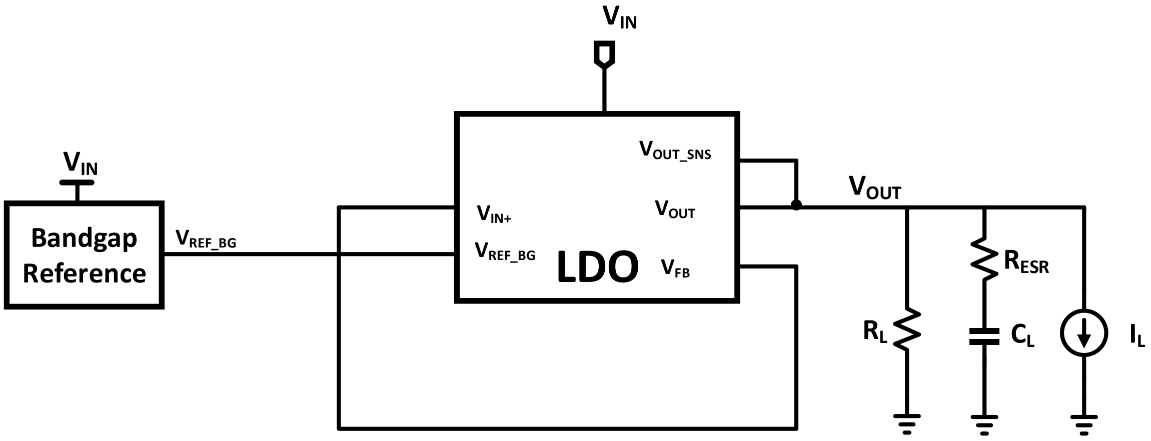


Figure 23: LDO Top Level Testbench

Figure 23 shows the top-level schematic of the designed LDO. Load capacitance of 1uF and equivalent series resistance (ESR) of 5m Ω are used. A bandgap reference circuit provides the reference voltage of 1.2V. The current load is realized by a resistive load of value Vout/Iload, and a step pulse current load is also attached for the transient response.

3.2.1 Understanding the Important Characteristics of the Designed LDO

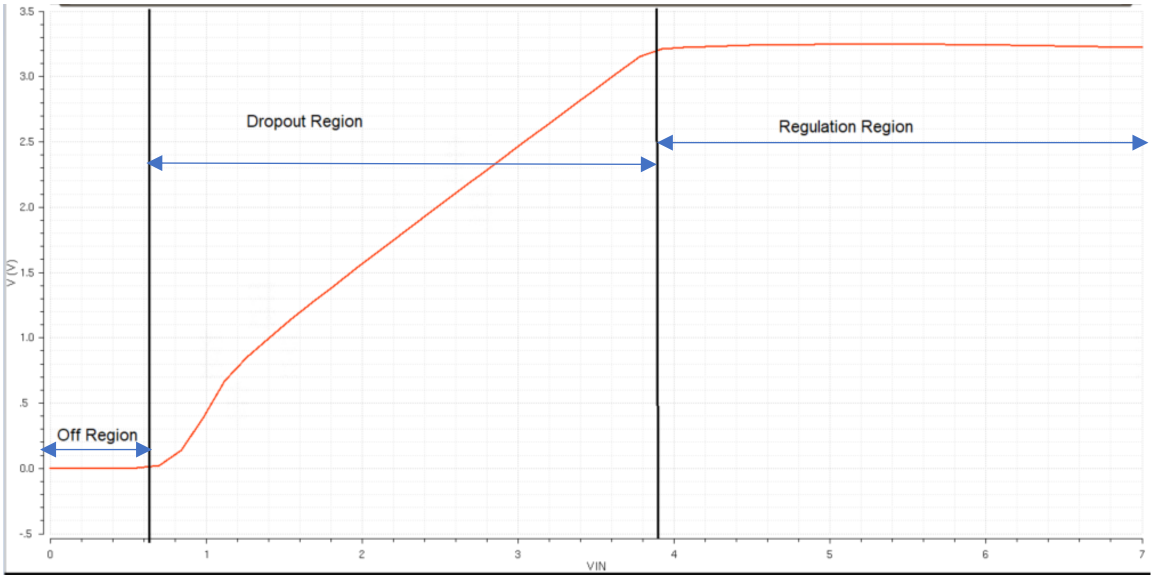
All the characteristics that are important to the LDO or defines the LDO are mentioned in this section.

3.2.1.1 Dropout Voltage

It is the minimum difference in input to output voltage of the LDO after which the circuit ceases to regulate. Linear voltage regulators require inputs which are higher than the rated output voltages. As the input voltage decreases towards the desired output voltage, it leads to condition of insufficient voltage which causes the regulator to drop out and provide unregulated output. More efficiency is achieved with the LDOs which have small voltage dropouts and able to provide stable voltage irrespective of load and line variations, temperature changes and time

Dropout region is when the pass transistor goes to linear region and acts as a resistor and dropout voltage is expressed as,

Vdropout=Ron.Ioad



Plot 1. Vout vs Vin of an LDO

In dropout region the PSRR is also affected severely, as the transistor is acting like a resistor. To Determine the dropout voltage, the LDO should be regulating at the maximum load current. If due to some malicious attack, the supply droops too low, it will either go to drop out or off region at a relatively higher voltage i.e. the regulation region width, as shown in plot1, will reduce.

Figure 24 shows a simplified schematic of an LDO. In dropout, the variable resistance is close to zero. The LDO cannot regulate the output voltage, so other parameters such as line-and-load regulation, accuracy, PSRR, and noise are meaningless.

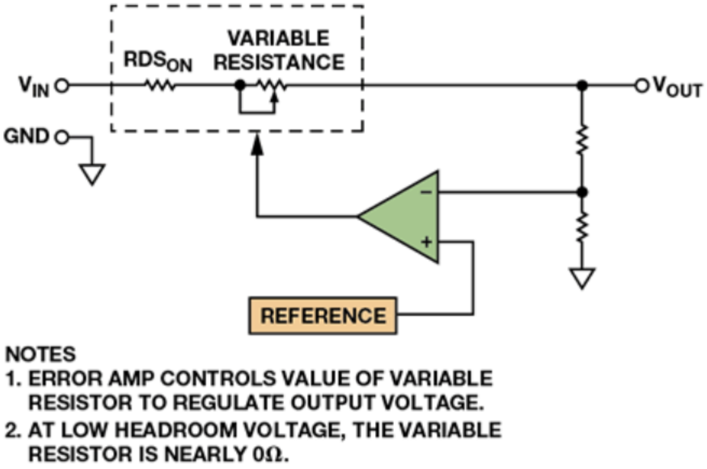
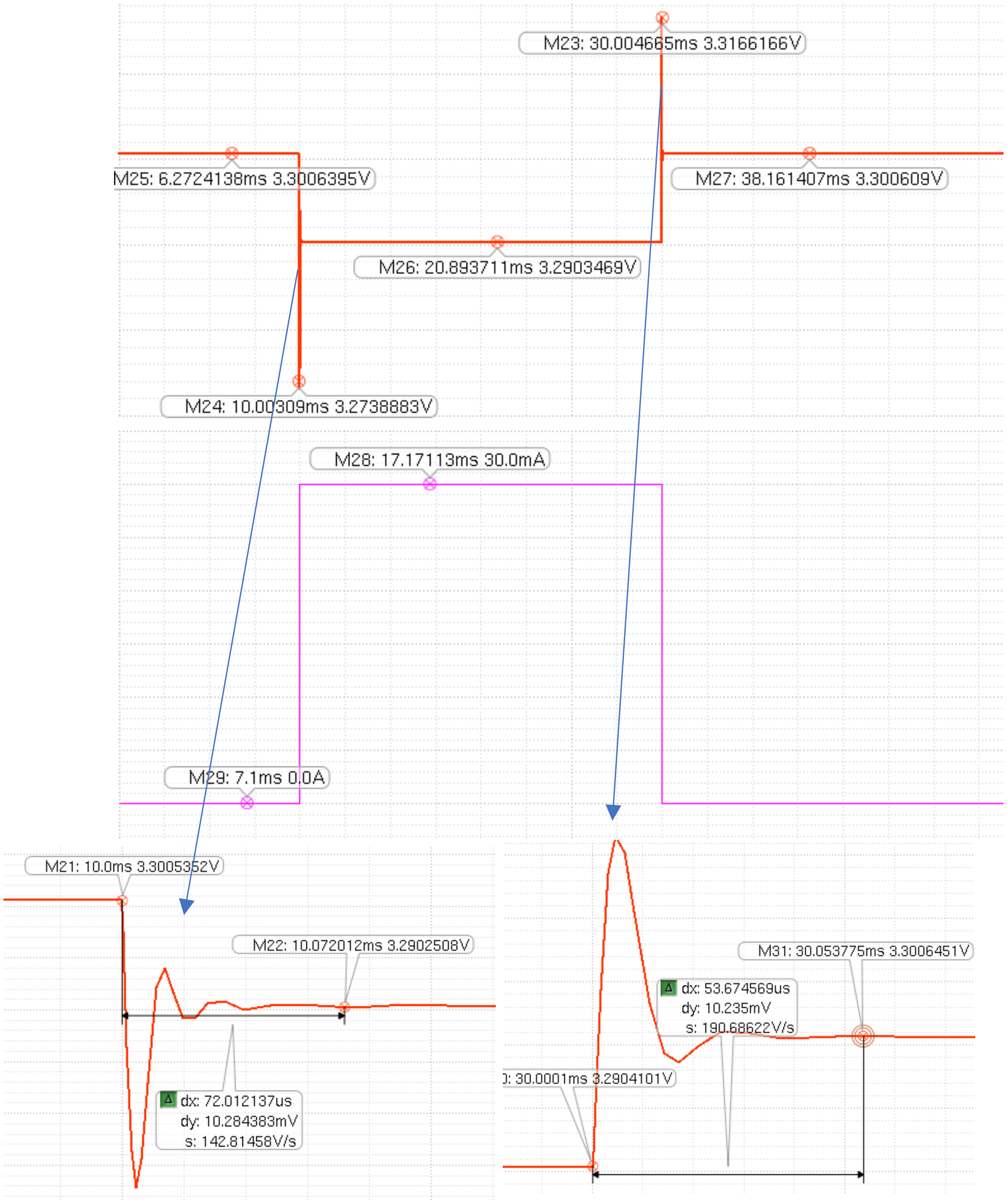

VARIABLE RESISTANCE
RDS$_{ON}$
V$_{IN}$
GND
V$_{OUT}$
–
+
REFERENCE
NOTES
1. ERROR AMP CONTROLS VALUE OF VARIABLE RESISTOR TO REGULATE OUTPUT VOLTAGE.
2. AT LOW HEADROOM VOLTAGE, THE VARIABLE RESISTOR IS NEARLY 0Ω.

Figure 24: Simplified Schematic of an LDO [26]

3.2.1.2 Transient Response

The transient response is determined by the maximum output voltage variation that is allowable when a step load change occurs. Due to the finite bandwidth of the feedback loop, the output voltage takes some time to sense the load change and correct against it.



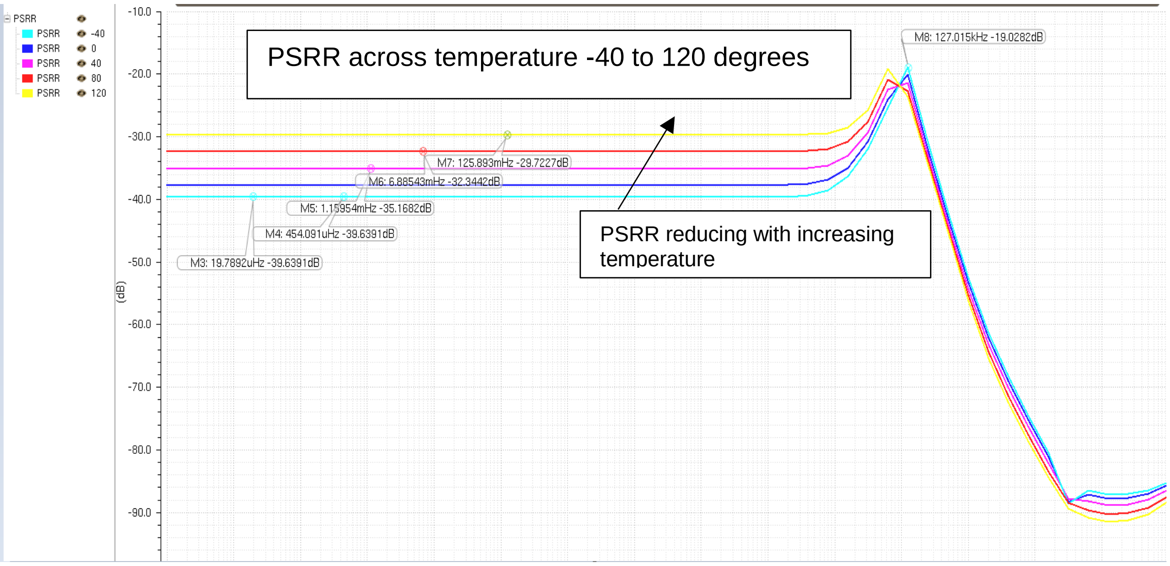
Plot 2. Transient Response of an LDO when a step load of 0 to 30mA is applied

It is a function of the load capacitor, the equivalent series resistance of the output capacitor, the bypass capacitor that is usually added to the output capacitor to improve the transient response.

Plot 2 shows the undershoot and overshoot when a step up or step down is applied, this is under nominal conditions and the undershoot is 2.1%, which is typically within specs. Ringing and a settling time of 72µs during step up and 54µs during step down is observed. To obtain a better transient response, a higher bandwidth of the LDO regulator, higher values of output/bypass capacitors, and low ESR values are recommended.

3.2.1.3 Power Supply Rejection

Power supply rejection ratio also known as ripple rejection quantifies the regulator's ability to reject the small signal noise from the supply nodes or it measures its ability to regulate the output voltage fluctuations caused by the input supply noise.



PSRR across temperature -40 to 120 degrees

PSRR reducing with increasing temperature

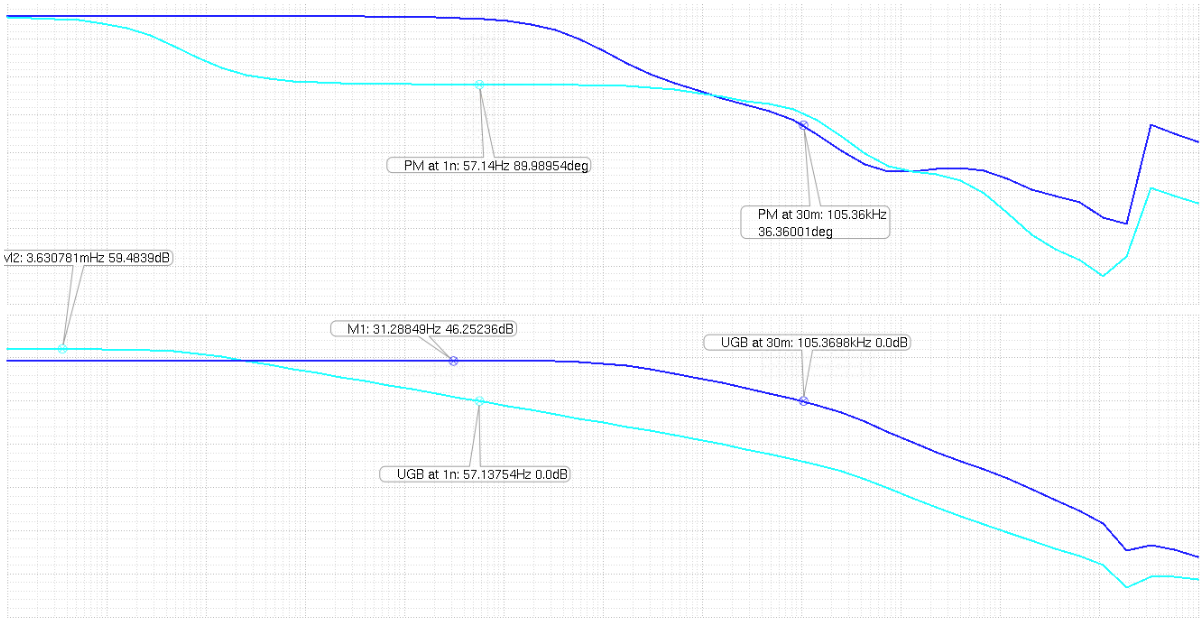
Plot 3. PSRR plots for temperature varying from -40 to 120 degrees

PSRR is directly dependent on the loop gain of the system, so it deteriorates at higher frequencies on encountering the dominant pole. It is usually defined by the product end and is usually at the higher load current as that's when the loop gain is less, and PSRR gets worse. Plot 3 shows the PSRR across a temperature range of -40 to 120 degrees, as the temperature increases the loop gain decreases and PSRR gets worse moving from 39dB to 29dB.

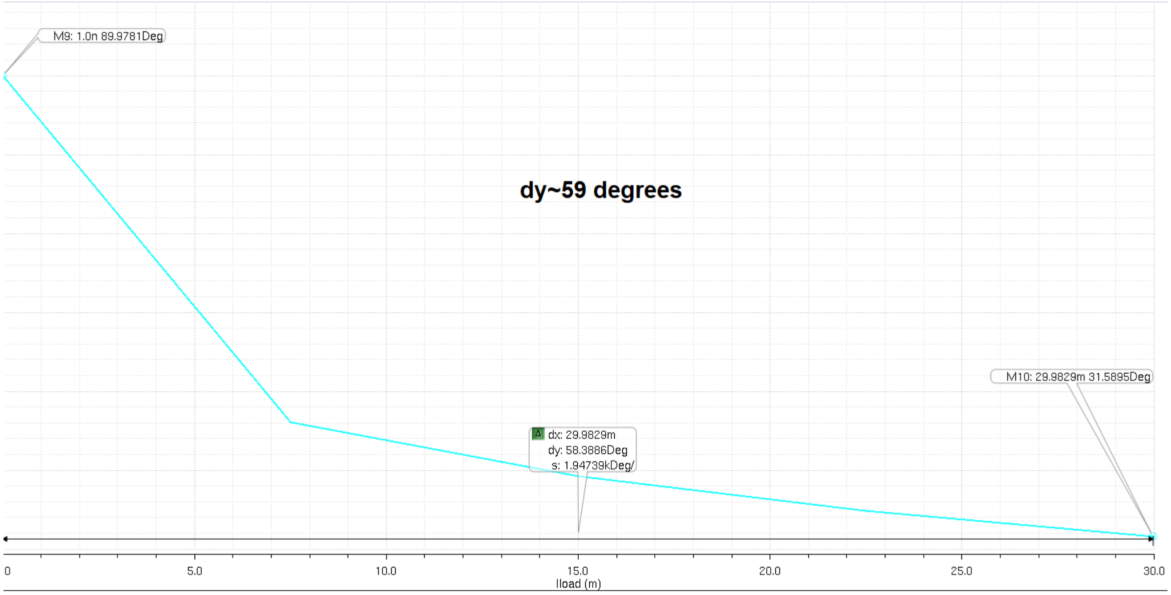
3.2.1.4 Stability and Phase Margin:

Although Phase margin does not have any hard specification from the product end, it depends on the designer's discretion. It is one of the most important property as many other parameters depend on it. If the LDO feedback loop ends up having more than 180 degrees of phase shift, it essentially acts as an oscillator and not LDO. Low phase margin can deteriorate the transient response and low loop gain can hamper the PSRR are DC accuracy of the LDO.

.



Plot 4. Loop gain and Phase Response at min (1nA) at max. (30mA) Load Current



Plot 5. Phase Margin with Respect to Load Current at Nominal Conditions

Plot 4 and 5 represent loop gain and phase for no load (1nA) and max load (30mA) conditions. dy represents the change in phase margin from minimum load to maximum load. Phase margin at low loads is almost 90 degrees as the dominant pole (output pole due to Cload) is at fairly low frequency but as the load current increases, the output poles moves higher in frequency as the impedance changes and gets closer to the second dominant pole (at the output of the error amplifier). Plot 5 represents the phase margin with respect to increasing load current, as expected the phase margin decreases with load current. Miller compensation is employed to compensate at high loads, the lead compensated LHP zero helps with the phase margin.

3.3 Motivation for BIST in an LDO

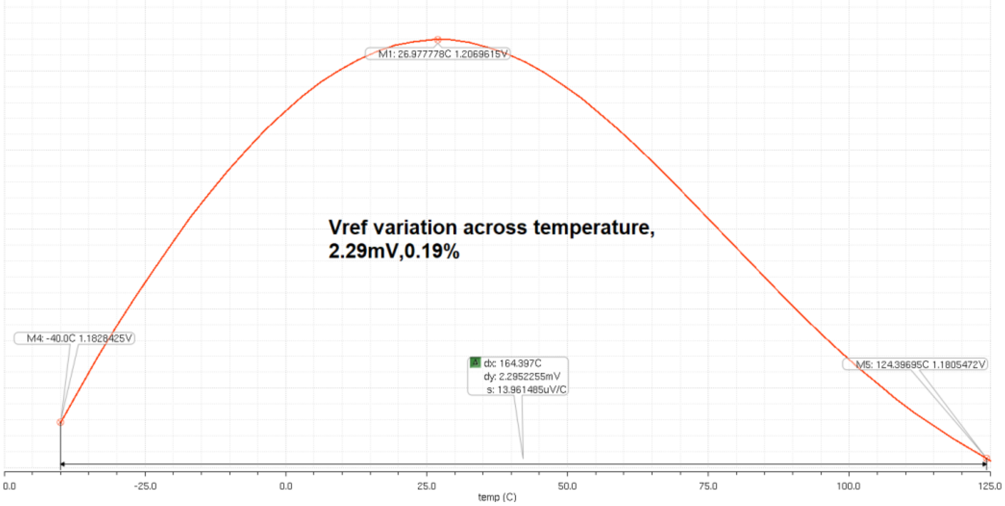
Although the LDO is an analog circuit, the control and different modes of operation typically require digital circuitry. Circuits like current mirrors and bandgap references are usually digitally calibrated, and digital circuits are more prone to attacks. This chapter would explore the effects that digital circuitry has on the functionality of an LDO. The attacks mentioned in section 1.4 can cause unpredictable bit flips in the digital control circuitry and may cause undesirable effects in the LDO performance. The output voltage might be within specifications which gives the impression that the LDO is successfully operating but an attack might cause the LDO to have a small phase margin which causes issues in transient response. Very small phase margin may cause the output voltage to ring for a long time (higher settling times), on the contrary very higher phase margin may cause the output response to be very slow. So, a method is needed to monitor the Phase margin while the LDO is operating in the field.

Types of Digital Controls in Analog Circuits:

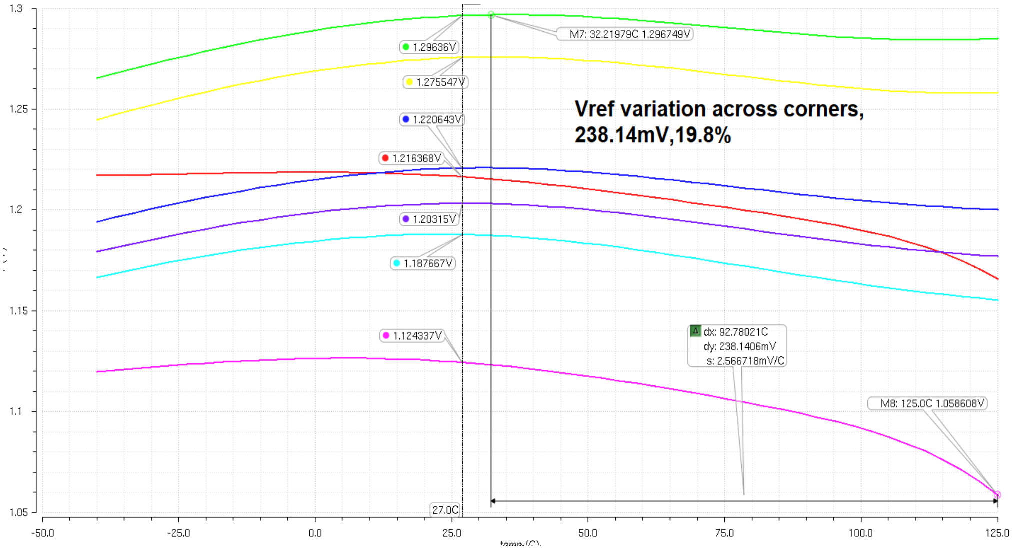
3.3.1 Trimming

Trimming is employed to fine-tune the output of a circuit. For instance, if a BGR that is supposed to have an output voltage of 1.2V but across process corners it varies by 5% i.e. ±60mV and as a system requirement it needs to be 1% accurate. A trimming circuit can be used to achieve the same. The trimming range should cover the variation due to process and mismatch. It uses switches and digital control to tune the output to an accurate value. The number of trimming bits needs to be calculated carefully. Too large trimming bits can cause increased complexity, increased trimming time and leakage through the switches. Too less causes low precision.

Plot 7 shows the BGR output voltage across temperature in typical corner and plot 8 shows variation across process corners. Figure 24 shows the Bandgap circuit designed, with trimming capability for resistor R0, as depicted in figure 25.



Plot 6. Vref Across Temperature



Plot 7. Vref Across Temperature in Process Corners

A trimming circuit needs to be designed that takes care of the 238.14mV variation across corners. Reference voltage from the below circuit can be derived as,

$$V_{REF\_BG} = R_0(\frac{V_{BE}}{R} + \frac{1}{R_1}\Delta V_{BE})$$

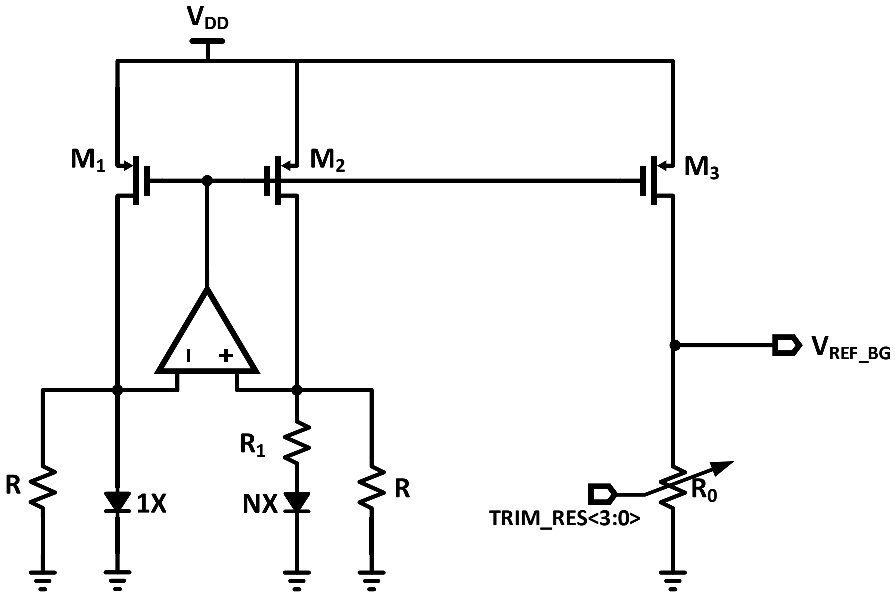


Figure 24: Bandgap Reference Circuit with Trimming Circuit Designed for R0

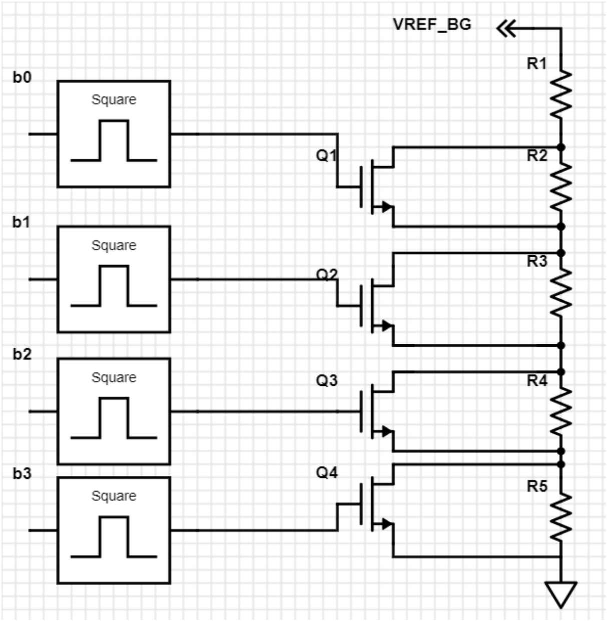


Figure 25: 4-bit Trimming Circuit for R0

For covering a range of 240mV with a resolution of 15mV:

$$\frac{\mathbf{240}\boldsymbol{mV}}{\mathbf{15}\boldsymbol{mV}} = \mathbf{16}$$

$$log_2(16) = 4\ binary\ bits$$

Each of the bits controlling the DC voltage sources are b0, b1, b2 and b3.

3.3.2 Programmability

This provides flexibility and reusability to a circuit. For instance, if an LDO that has an output of 3.3V but the output voltage can be altered, this is a type of coarse tuning. The resistor divider can be controlled by switches and digital control to change the output voltage. In figure 27, a programmable resistor string is utilized for multi-output, and a tunable resistor ladder is introduced in the feedback network for high-precision LDO output control. The resistor divider is realized using switches and has multiple tap points for different voltages. R1 shown in figure 26 is broken into smaller resistances with multiple tapping points. When (V1.V2.V3.V4)=0001, Vout=3.3V (Nominal).

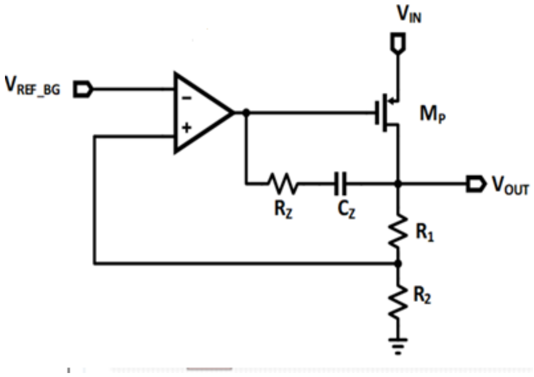


Figure 26: LDO Architecture with Miller Compensation

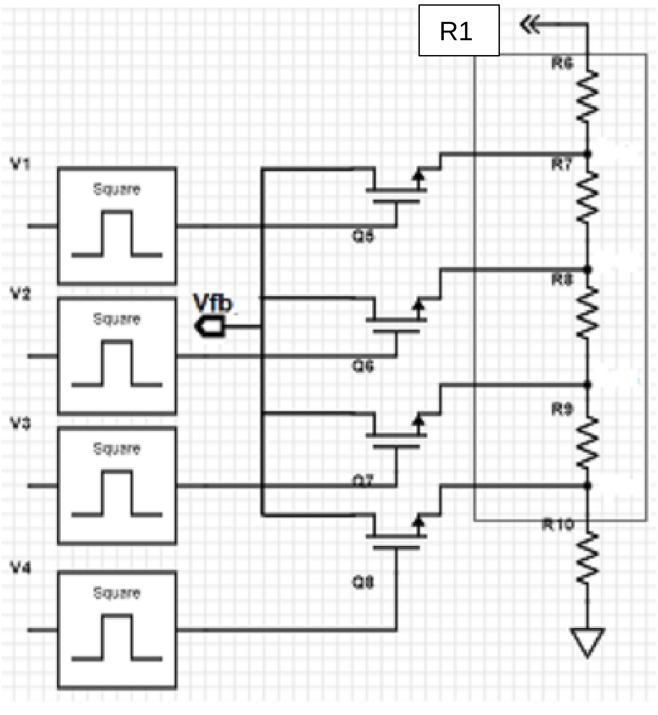


Figure 27: Programmability Realized by having Multiple Tap Points for R1

3.3.3 Adaptive Biasing

To reduce the quiescent current requirement, Adaptive biasing is employed widely in circuits nowadays. In this method, the bias current is composed of a fixed biasing current Ibias and an adaptive feedback current IAB as shown in figure 28. At heavy load, the feedback current IAB increases the error amplifier biasing current, which extends the loop bandwidth; at light loads, the low fixed current Ibias maintains high current efficiency [25]. A biasing circuit that can deliver a load current of 100 mA at a dropout voltage only consumes a quiescent current of 7 μA at light loads [24]. Adaptive biasing can provide other features such as higher loop gain, faster transient response, and better power supply rejection than fixed biasing. In adaptive biasing, as the load current is increased the other bias currents are also boosted which results in a system, where the poles track each other resulting in a potential higher bandwidth system. In [25] the author has achieved an LDO regulator with 34dB higher loop gain, 46% faster transient response, and about 12dB higher power supply rejection above 1MHz than the one with fixed bias. If the control is digital to sense the low load current mode and switch to a low quiescent current, there is a possibility of being hacked and the LDO might be in a low quiescent current mode in moderate of high load conditions, which can cause a multitude of problems.

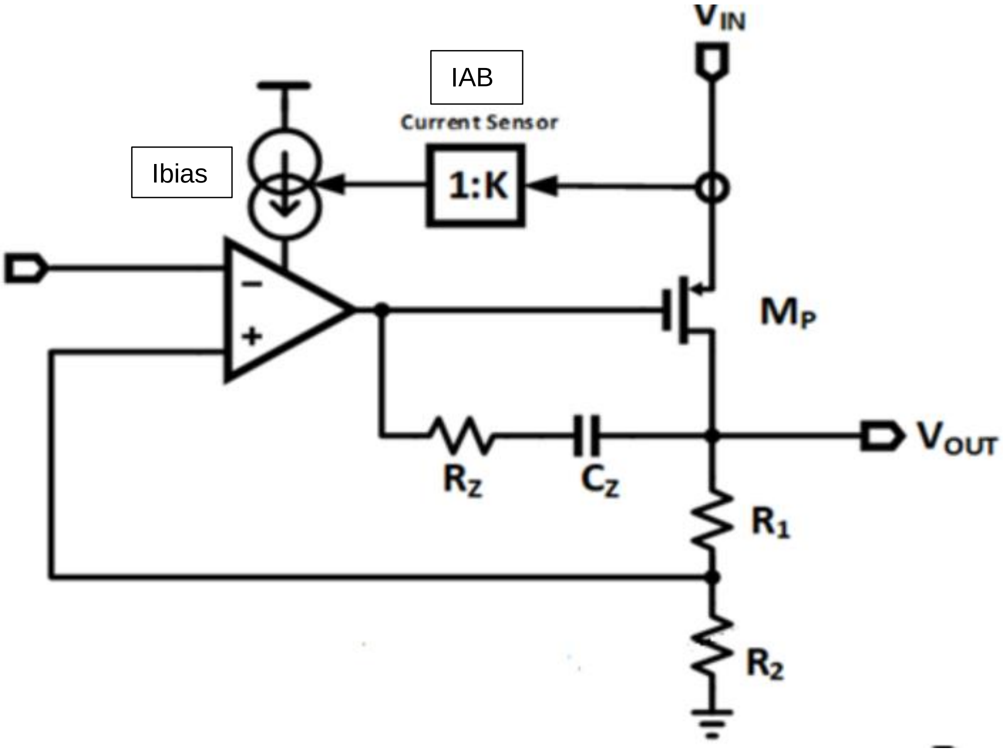
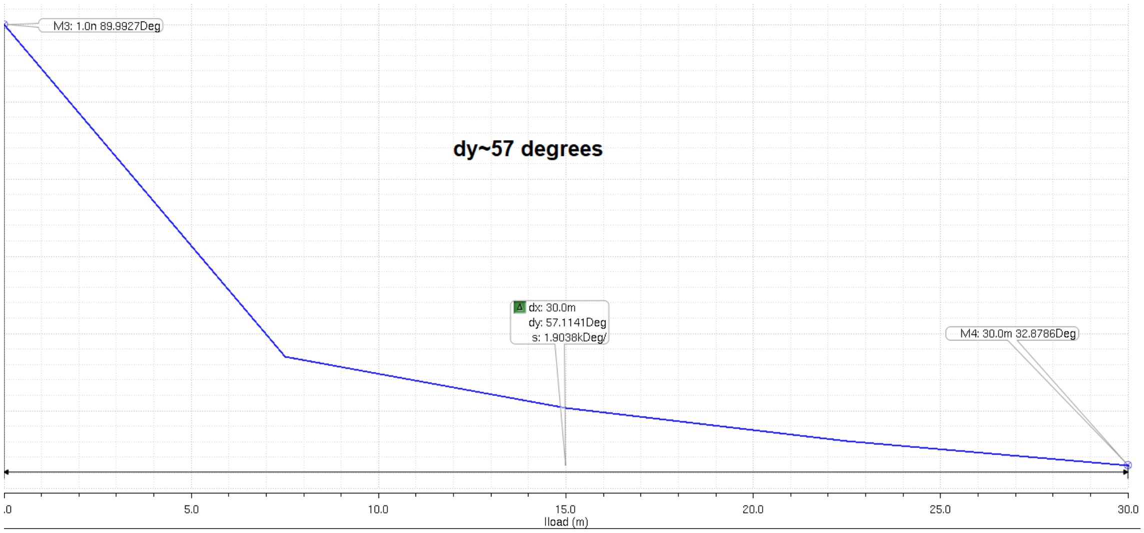


Figure 28: LDO with Adaptive Biasing

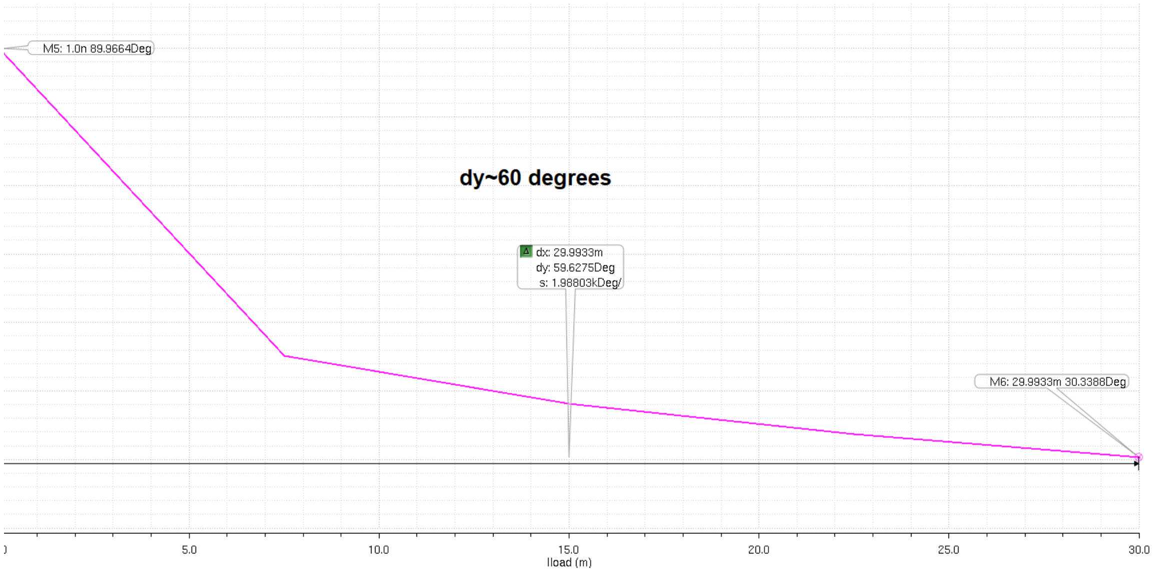
3.4 Effect of Digital Controls on LDO Characteristics

3.4.1.1 Trimming

The trimming bits are varied from 1111 to 0000, i.e. all the bits are flipped, and the phase margin variation is measured. Nominal BGR trim bits are 1110.



Plot 8. Phase Margin Across Varying Load Current for b0 b1 b2 b3 = (1111)



Plot 9. Phase Margin Across Varying Load Current for b0 b1 b2 b3 = (0000)

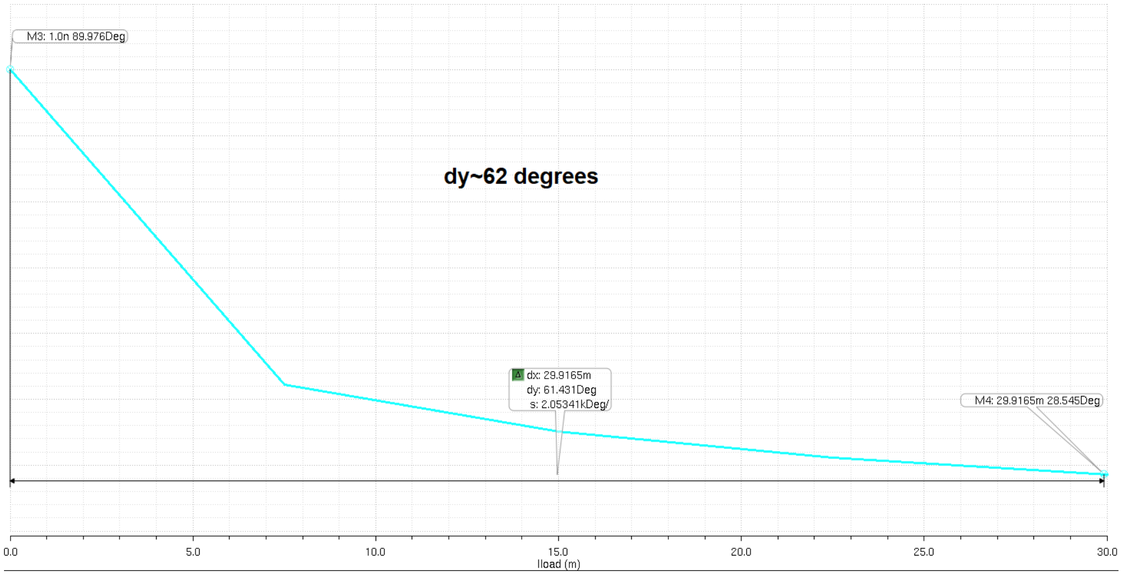
Where dy represents the change in Phase Margin when the LDO is subjected to varying load condition, from minimum to maximum.

There is not much variation in Phase Margin for both the cases as shown in plot 9 and 10, controlling the trim bits will only change the DC value of the Vref, which affects the DC accuracy of the LDO but negligible effect on the phase margin.

3.4.2 Programmability

The nominal output voltage was 3.3V or when V4=1, here V1=1 is supplied and the phase margin variation is observed.

For (V1.V2.V3.V4) =1000,



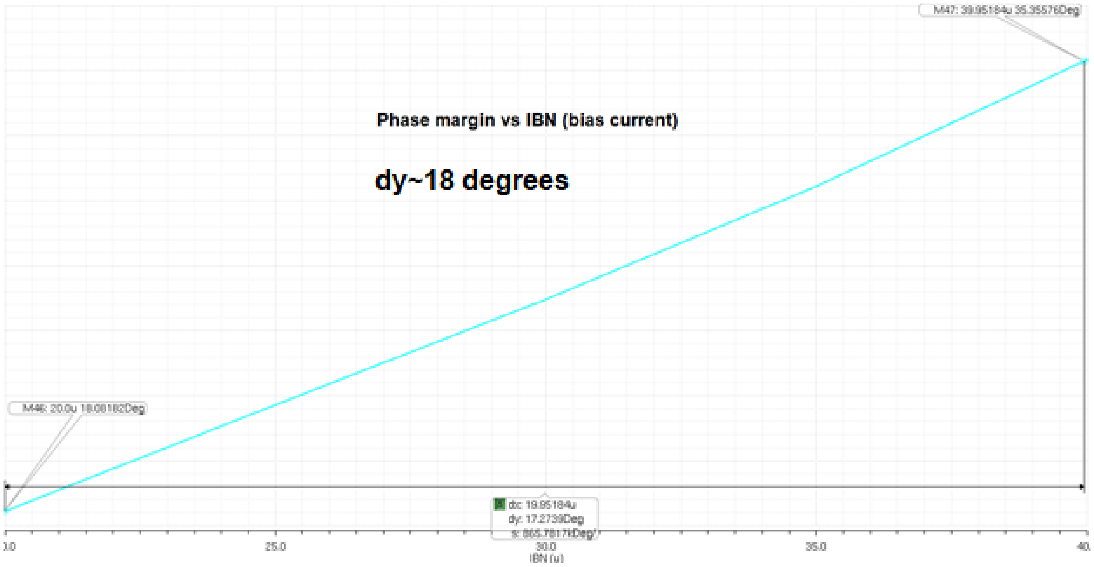
Plot 10. Phase Margin Across Varying Load Current for V1=1 mode

Plot 11 shows the Phase margin with respect to the load current. As the load current is increased the output pole moves higher in frequency, moving closer to the error amplifier pole, reducing the phase margin.

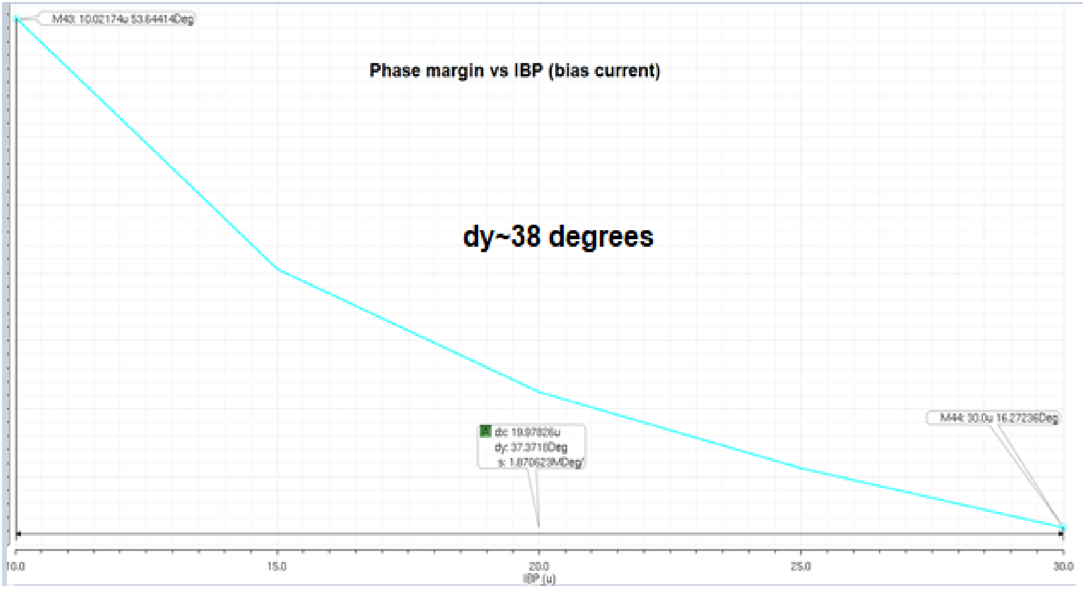
Plot 5 shows the phase margin variation at nominal conditions when V4=1, and the change in phase margin (dy) was observed to be 59 degrees. There is not much difference in phase margins for both the output voltage modes V1 and V4, as nothing has been changed in the circuit apart from the resistor divider ratio.

3.4.3 Adaptive Biasing

From figure 28, changing the nominal value of IBP (20uA) and IBN (30uA) by ±10uA. Plots 11 and 12 show the dependence of the phase margin on bias currents IBN and IBP.



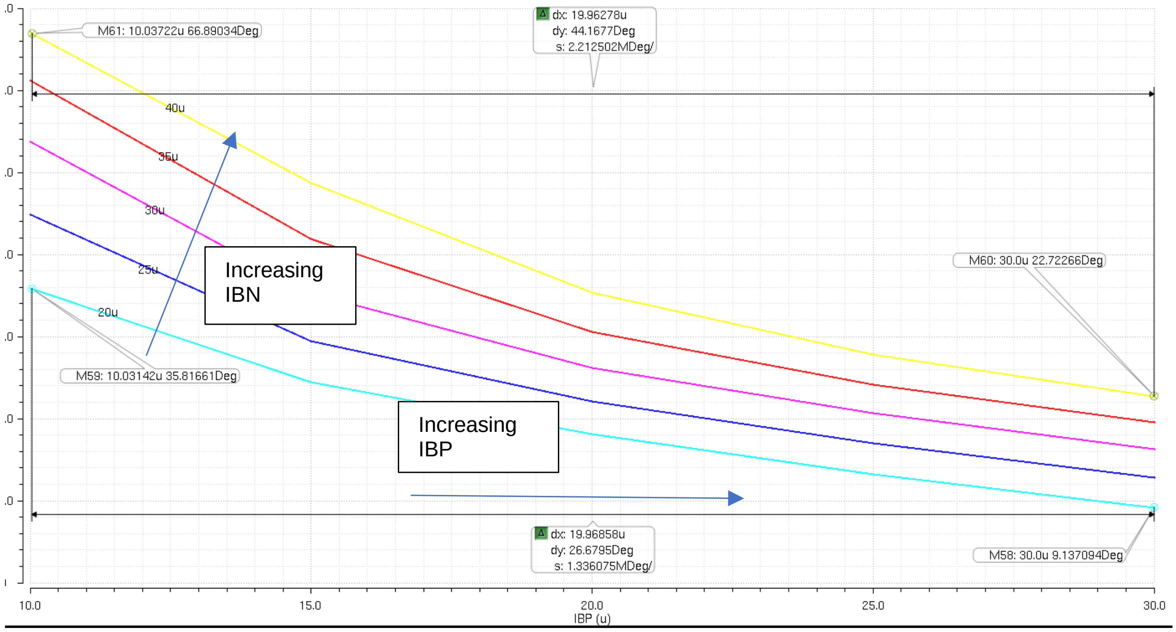
Plot 11. Phase Margin Across Varying IBN



Plot 12. Phase Margin Across Varying IBP

IBP controls the bias voltage of tail current devices of the error amplifier and hence has a greater effect of the phase margin the IBN, which just controls the bias voltage of cascode and tail devices.

As seen from the curves the phase margin increases with IBN and decreases with IBP, so minimum phase margin will be at minimum IBN and maximum IBP as shown below,

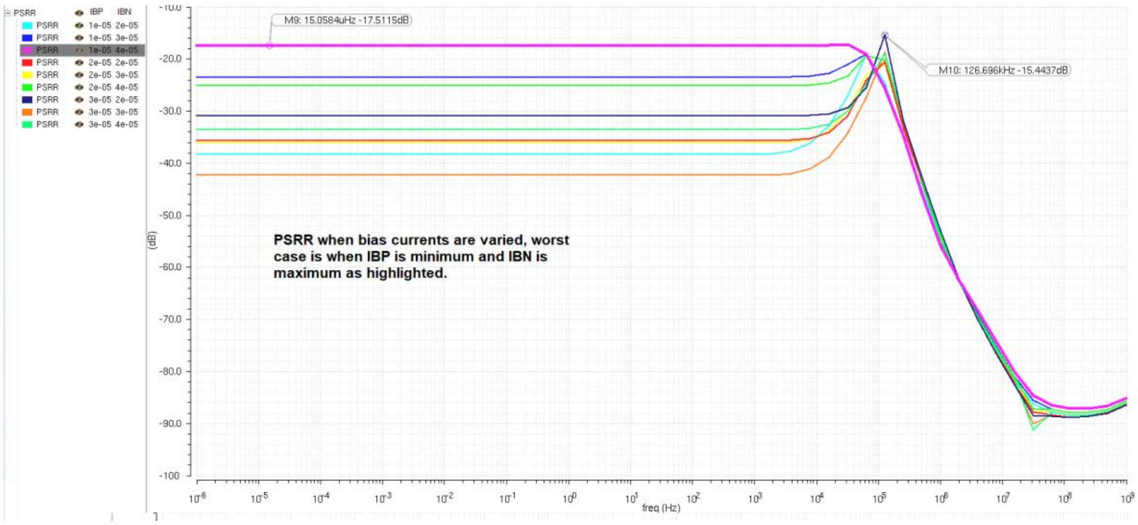


Plot 13. Phase Margin Variation When IBN and IBP (Bias Currents) both are Varied Simultaneously

Increasing or decreasing both the bias currents together helps a little with variation in phase margin as both has opposite effects, although they don't affect the phase margin with same the magnitude. Phase margin is more sensitive to IBP.

Adaptive Biasing caused the maximum Phase Margin variation. Subsequent plots represent PSRR and Transient response of an LDO when the Adaptive Biasing is malfunctioned due to a security attack.

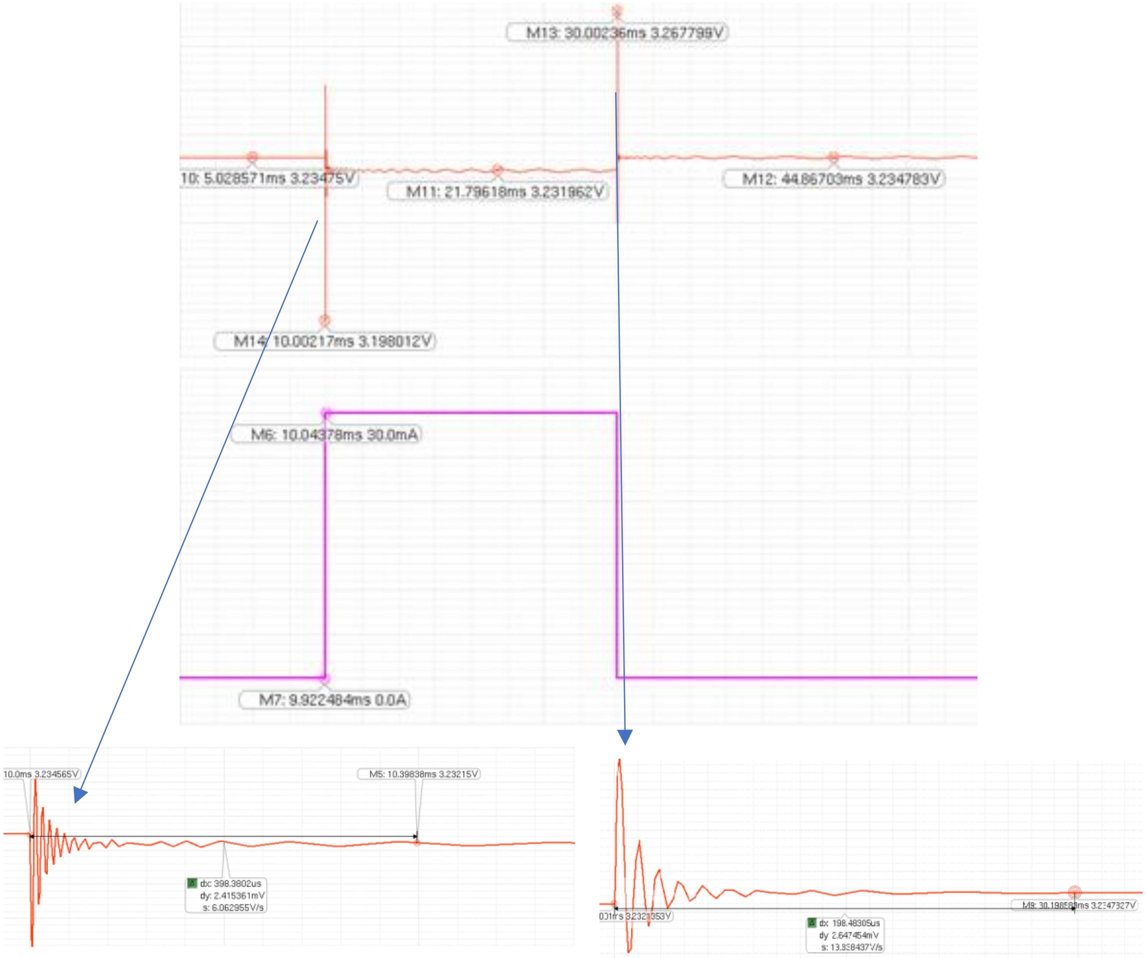
3.4.3.1 Effect on PSRR



Plot 14. PSRR Across Frequency When Bias Currents are Varied

PSRR is dependent on the bias currents supplied to the error amps as the total loop gain is dependent on that, and we see a worst case at IBP minimum and IBN maximum.

3.4.3.2 Effect on Transient Response



Plot 15. Transient Response at Maximum IBP and Minimum IBN

Plot 15 shows the transient response of the LDO for step load of 0 to 30mA, at minimum IBN and maximum IBP. Although the output voltage is within specs ~2%, the settling time has increased by 326µs (450%) for Step up and 144µs (266%), which can cause timing errors and hence potential system failure.

3.5 Determination of the Phase Margin from Impulse Response

The PRBS noise is injected at the Vref of the LDO, to maintain its closed-loop operation and correlation is done at the output of the LDO. BIST circuit measures the impulse response in the time domain. LDO stability parameters, such as phase margin, can be calculated based on the impulse response. Once the impulse response has been obtained we can estimate Phase margin from it which will indicate stability. The LDO typically is a second order system although time-domain analysis of the dynamic loop characteristics of higher order systems (3rd order or ore) is a non-trivial problem, the theory for 1st and 2nd order system has already been developed [22]. Damping ratio is a measure of how oscillations in a system decay after a disturbance is injected. The damping ratio is a system parameter, denoted by ζ (zeta), that can vary from undamped (ζ = 0), underdamped (ζ < 1) through critically damped (ζ = 1) to overdamped (ζ > 1).

Depending on the type of damping the system represents, there are different analytical method to estimate the damping ratio and hence the phase margin.

Overdamped System:

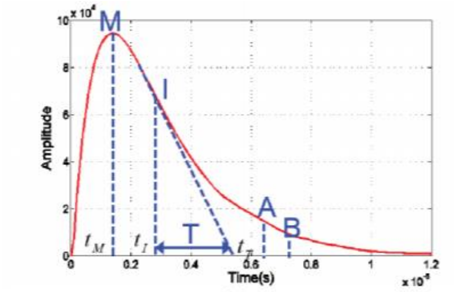


Figure 29: Overdamped Response [23]

$$\mathit{Overdamped}: \; \zeta = \frac{T\omega_1}{2\sqrt{T\omega_1 - 1}}$$

$$\left(\omega_1 = \frac{1}{\Delta t}\ln(x_A/x_B)\,, \Delta t = t_B - t_A\right)$$

Where $t_A$and x_A are time and amplitude at A respectively while and t_B are x_B time and amplitude at B respectively as depicted in the diagram [23].

Once we have the damping ratio, the phase margin can be estimated as,

$$\Phi_M = \tan^{-1}\left(\frac{2\zeta}{\sqrt{-2\zeta^2 + \sqrt{4\zeta^4 + 1}}}\right)$$

Underdamped System:

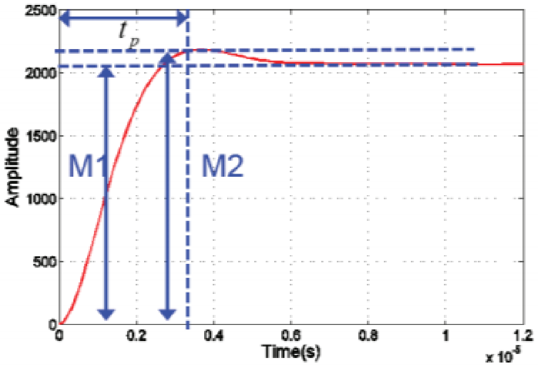


Figure 30: Underdamped Response [23]

$$Underdamped : \zeta = \sqrt{\frac{1}{1 + (\pi/\ln M)^2}}$$

Where M= $(M_2$- $M_1)/M_1$ and M_1 is the magnitude at the steady state and M_2 is the peak amplitude [23].

3.6 Conclusion:

Analog circuits have some control features that are digital and are prone to security attacks as discussed in previous sections. This chapter describes how it affects the analog part of the LDO. An LDO with typical characteristics and a load capacitance of 1µF was designed. The digital controls that these circuits typically have are trimming, programmability and adaptive bias currents. These controls were manually varied in a way, it would be affected when under a security attack and the performance parameters were measured before and during an attack.

- Programmability does not affect the analog performance to a great extent, we saw 4 degrees change in phase margin at nominal conditions, although if the LDO is not pre-designed for a sufficient phase margin, it might affect the performance.
- Trimming bits of the BGR alters the DC accuracy of the LDO but not the Phase margin to a great extent.
- Adaptive biasing, on the other, hand may affect the LDO performance severely as shown in section 3.4.3.

If the control is hacked which ends up increasing one and decreasing the other bias current higher settling times and ringing is observed in the response which may cause a timing error. A PRBS signal can be injected in the LDO control loop and can be correlated with the output to estimate the impulse response which in turn provides us with the phase margin. The phase margin indicates the stability which in turn affects the transient response. So, instead of trying to decode or prevent a particular type of attack, the LDO is monitored for its overall performance, which will indicate the presence of a malicious circuit.

REFERENCES

[1] Fundamentals of Power electronics, Robert Erikson, Dragan Maksimovic.

[2] N.Beohar et al.,"Disturbance-free BIST for loop characterization of DC-DC buck converters," 2015 IEEE 33rd VLSI Test Symposium (VTS), Napa, CA, 2015, pp. 1-6.

[3] C. Shi, B. C. Walker, E. Zeisel, B. Hu and G. H. McAllister, "A Highly Integrated Power Management IC for Advanced Mobile Applications," in IEEE Journal of Solid-State Circuits, vol. 42, no. 8, pp. 1723-1731, Aug. 2007.

[4]"Aluminum electrolytic capacitors," EPCOS datasheet, Available: http://www.epcos.com/inf/20/30/db/aec_07/B43305.pdf, Oct. 2007

[5] "Type MLP Aluminum Capacitors," datasheet, Available: http://www.cde.com/catalogs/MLP.pdf

[6] J. A. Morroni. Adaptive tuning and monitoring of digitally controlled switched mode power supplies, 2009

[7]] Power Management IC (PMIC) Market by Product (Linear Regulator, Switching Regulator, Voltage References, Battery Management IC, Energy Management IC, LED Driver IC, POE Controller, Wireless Charging IC), Application, and Geography - Global Forecast to 2022 Available: https://www.marketsandmarkets.com/Market-Reports/power-management-ic-market-441.html

[8] APPLICATION NOTE 6857,Addressing the Challenges of High-Voltage Automotive Power Applications, Chintan Parikh and George Chen https://www.maximintegrated.com/en/app-notes/index.mvp/id/6857

[9] Small-Signal MATLAB/Simulink Model of DC-DC Buck Converter using State-Space Averaging Method, M. S. Hassan,Adel A.Elbaset

[10] L. Ljung, System Identification: Theory for the User, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1999.

[11] K. R. Godfrey, "Introduction to binary signals used in system identification," in Proc. IEEE Int. Conf. Control, vol. 1, 1991, pp.161-166

[12] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1283-1295, Aug. 2014. doi: 10.1109/JPROC.2014.2335155

[13] J. A. Kash, J. C. Tsang, and D. R. Knebel, Method and apparatus for reverse engineering integrated circuits by monitoring optical emission, US Patent US6496022 B1, 2002.

[14] F. Koushanfar and A. Mirhoseini, ‘‘A unified framework for multimodal submodular integrated circuits trojan detection,’’ IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 162–174, Mar. 2011.

[15] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, ‘‘Trustworthy hardware: Identifying and classifying hardware trojans,’’ IEEE Computer, vol. 43, no. 10, pp. 39–46, Oct. 2010.

[16] M. Tehranipoor and F. Koushanfar, ‘‘A survey of hardware trojan taxonomy and detection,’’ IEEE Design Test Comput., vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010.

[17] TPS62748 (ACTIVE) High-efficiency Buck Converter with Ultra-low Quiescent Current and Load Switch http://www.ti.com/product/TPS62748

[18] Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review) Mark Beaumont, Bradley Hopkins and Tristan Newby

[19] N. Beohar, V. N. K. Malladi, D. Mandal, S. Ozev and B. Bakkaloglu, "Online Built-In Self-Test of High Switching Frequency DC–DC Converters Using Model Reference Based System Identification Techniques," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 2, pp. 818-831, Feb. 2018.

[20] Mohammad Al-Shyoukh, Hoi Lee and Raul Perez, “A Transient-Enhanced Low-Quiescent Current Low-Dropout Regulator with Buffer Impedance Attenuation”, IEEE, JOURNAL OF SOLID-STATE CIRCUIT, VOL.42, NO.8, 2007(8) pp. 1732-1742.

[21] “A programmable multi-output technique in LDO regulator for multi-reference SAR ADC application” Xingyuan Tong & Tiantian Sun

[22] K. Ogata, Modern Control Engineering, 4th ed. Upper Saddle River, NJ:
Prentice-Hall, 2002.

[23] J. W. Jeong, E. Yilmaz, L. Winemberg and S. Ozev, "Built-in self-test for stability measurement of low dropout regulator," *2017 IEEE International Test Conference (ITC)*, Fort Worth, TX, 2017, pp. 1-9.

[24] X. Ming, Q. Li, Z. Zhou and B. Zhang, "An Ultrafast Adaptively Biased Capacitorless LDO With Dynamic Charging Control," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 1, pp. 40-44, Jan. 2012.

[25] X. Han, T. Burger and Q. Huang, "An output-capacitor-free adaptively biased LDO regulator with robust frequency compensation in 0.13µm CMOS for SoC application," *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, 2016, pp. 2699-2702.

[26]Understand Low-Dropout Regulator (LDO) Concepts to Achieve Optimal Designs https://www.analog.com/en/analog-dialogue/articles/understand-ldo-concepts.html