3-2023

Assessing Hardware Security Threats Posed by Hardware Trojans in Power Electronics

Quinn Kinzie
qkinzie@clemson.edu

Assessing Hardware Security Threats Posed by Hardware Trojans in Power Electronics

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Electrical Engineering

by
Quinn Kinzie
May 2023

Accepted by:
Dr. Yingjie Lao, Committee Chair
Dr. Zheyu Zhang
Dr. Christopher Edrington

Abstract

This study investigates the threat of hardware Trojans (HTs) in power electronics applications, a rising concern due to the growing demand for cost-effective embedded solutions in power systems. With the supply chain for electronic hardware devices expanding globally, particularly to low-cost foundries in foreign locations, there is an increasing risk of HT attacks. While there has been extensive research on HTs in computer applications, little consideration has been given to their threat in power electronics. This study demonstrates the effectiveness of a power electronics HT by implementing a novel HT design into a gate drive circuit. Additionally, the research proposes several HT designs that exploit factors unique to power circuits, such as high power delivery and analog circuitry in order to illustrate the distinct attack space. The research highlights the need for enhanced detection, protection, and prevention methods in power electronics applications and offers a roadmap for future studies to develop more effective countermeasures and algorithms to mitigate the risks of HT attacks in power electronics.

Acknowledgments

I would first like to thank my advisor Dr. Yingjie Lao for his support throughout the whole process of conducting research and writing this thesis. He has always been available when I needed help, and I have benefited greatly from his expertise and his kindness.

I would also like to express my gratitude to Dr. Zheyu Zhang and Dr. Christopher Edrington for not only serving on my committee, but also for making themselves available to me throughout the year. They have generously provided me with research insight and moral support that has proven invaluable to my success.

Lastly, I want to thank my dad for being a constant source of help and wise counsel to me in navigating graduate school, as well as my mom and the rest of my family for their encouragement and unconditional support throughout the process of writing this thesis. This would not have been possible without them.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Hardware Security

Power electronics are rapidly evolving with the integration of computers and electronics in embedded systems, a revolution driven by the Internet of Things (IoT). Power systems are being enhanced with unprecedented computational power. Meanwhile, the migration to network-enabled monitoring systems and control approaches is connecting power electronic devices all over the world [1–3]. This transformation is impacting a diverse range of technological industries, ranging from life-saving medical devices to cutting-edge military operations [4–7]. Due to the widespread use of hardware devices in critical systems, hardware security has become an increasingly important research area. Contrary to the remote nature of cyberattacks, hardware attacks occur within the physical system, presenting adversaries with another avenue for attacks distinct from the software and network domains [8].

In order to employ a hardware attack, the attacker must have physical access to the victim's device at some point in its life cycle. However, as the supply chain for electronic hardware devices expands globally to include low-cost foundries in foreign locations, the opportunities for attacks are also increasing. This is because electronic components become more accessible and vulnerable to exploitation, allowing untrusted actors to infiltrate the supply chain and introduce malicious hardware or software [9, 10]. This shift in design flow can be attributed to the trend of shrinking transistor technologies and increasingly complex device fabrication, which have driven up manufacturing costs [11]. In order to remain competitive in the dynamic market, companies outsource some stages of device production to third-party vendors in low-cost countries where trust has yet to be established. Intellectual property (IP) theft can occur, by which untrusted parties can abuse their access to client IP by stealing ideas and implementing them for commercial gain [12]. Additionally, untrusted fabrication centers may engage in covert overproduction of electronic devices, which they can sell at a profit without incurring any design costs [13].

1.2 Hardware Trojans

In addition to theft, an adversary with access to the device can execute various nefarious attacks, such as mechanical damage, intellectual property theft, and reverse engineering. Furthermore, if they obtain the device netlist before production, they can insert hidden, malicious circuitry known as a hardware Trojan (HT) to compromise device security and functionality. Hardware Trojans are particularly common in integrated circuits (ICs), which are used in power electronics for processing information and controlling other devices [14]. Due to their compact and complex design, ICs are frequently outsourced to third-party vendors for manufacturing, making them prime targets for hardware Trojan attacks [15]. The HT architecture can be decomposed into a trigger and a payload, as shown in Fig. 1.1. The trigger relies on a specific input combination or rare event to determine when the Trojan will be activated, while the payload is the malicious behavior the Trojan delivers to the system.

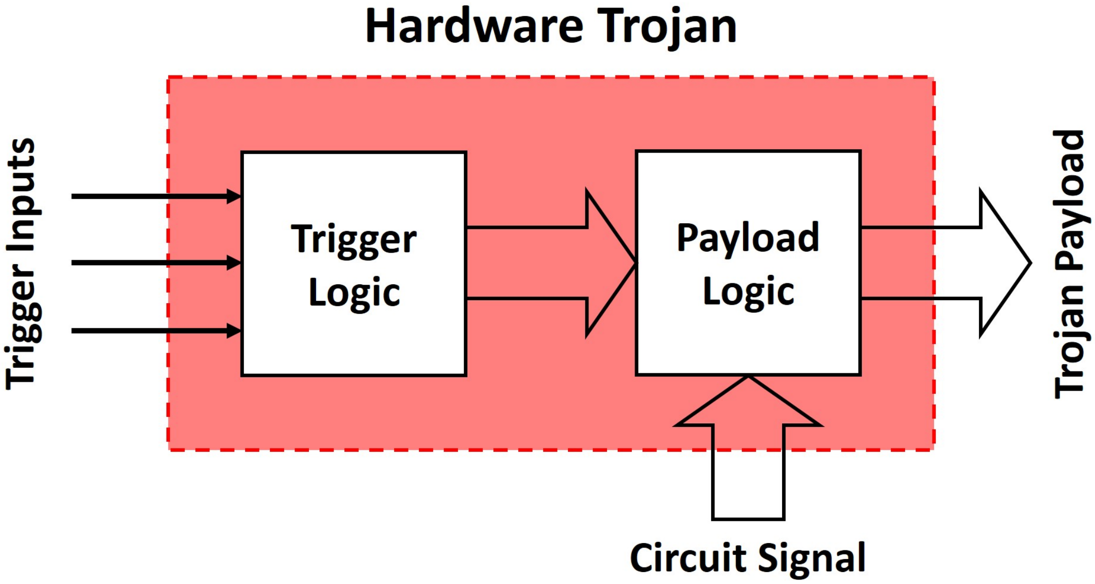


Figure 1.1: Hardware Trojan Architecture

1.3 Research Motivation

While there is substantial research into HTs in computer applications and various publications outlining HT detection and protection approaches [16, 17], there has been little consideration in the academic community of their threat within power electronics applications. As a result, there are few, if any, publications on the topic. This thesis explores the novel and unexplored research space of HTs designed to target power electronics and investigates two main research objectives. The first was to demonstrate the effectiveness of a power electronics HT, achieved through the design, implementation, and analysis of a novel and functional power electronics HT inserted into a gate drive IC. The second objective was to shed light on the vulnerabilities and scope of the attack space in the gate drive IC, accomplished by proposing several HT payload and trigger designs that are viable for implementation in the gate drive IC. The purpose of this research is to demonstrate and assess the viability of HT attacks in power electronics, with the goal of advancing HT detection, protection, and prevention methods for power electronics applications.

This thesis is organized as follows: Chapter 2 provides an overview of HT attacks, details previously proposed HT detection methods, and argues for the importance of developing such approaches for power electronics applications. Chapter 3 outlines the methodology of this study. Chapter 4 describes the implementation and analysis of a novel power electronics HT designed to attack the gate drive IC's fault protection circuitry. Chapters 5 and 6 propose several HT payloads and triggers designed for the gate drive IC, addressing the implementation efficacy and limitations of each attack. Finally, research conclusions and future work are discussed in Chapter 7.

Chapter 2

Background

2.1 Threats in the Supply Chain

The widespread implementation of electronic hardware has led to the development of various types of hardware attacks that can compromise a system's functionality or privacy, including physical damage, reverse engineering, piracy of IP, and hardware Trojans [18–20]. Given the variety of potential attacks, companies must be mindful of hardware threats at every point in the product lifecycle, all the way through design, fabrication, application, and disposal. Fig. 2.1 highlights some of the most significant hardware security threats at each stage in the product lifecycle.

2.2 Hardware Trojans

A hardware Trojan refers to malicious circuitry that is discretely inserted into an existing circuit during the design or manufacturing stage of production. The HT architecture is composed of two parts: a trigger and a payload. Under normal operating conditions, the HT remains dormant and does not affect the behavior of the circuit. However, once the Trojan is triggered, the payload executes malicious activity within the circuit. Sections 2.3 and 2.4 examine hardware Trojan payloads and triggers, respectively, providing an overview of their taxonomy and detailing examples of their implementation.

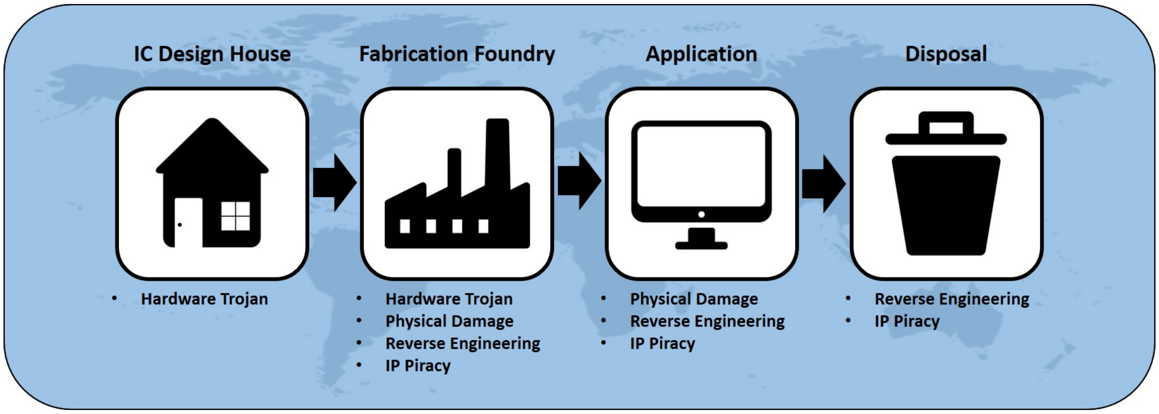


Figure 2.1: Security threats at each stage in the product lifecycle

2.3 Payload

The payload of the HT is the malicious behavior performed by the HT within the compromised circuit. The payload mechanism must be implemented stealthily into the device so that it is challenging to identify by physically inspecting the hardware. It is also essential that the payload's behavior is not evident during standard functionality so that it will be undetectable during pre-implementation testing. Attackers accomplish low detectability in the HT design by employing a trigger mechanism. The payload remains dormant until triggered, meaning that the trigger mechanism must isolate the payload function from the standard functionality of the circuit. Once triggered, the payload performs malicious actions based on the attacker's intention. Three common goals of HT payloads are to compromise functionality, damage circuitry, or leak sensitive information. This taxonomy and numerous HT benchmarks are details in a database provided by Trust-Hub [21, 22], a resource sponsored by the National Science Foundation to facilitate research and technology development in the domain of hardware security. Many of the HT examples described below will be drawn from this database.

Payloads that ***compromise functionality*** may include denial-of-service or altering a system function [23–25]. For example, a denial-of-service attack was designed to disable a medical implant device by activating a continuous shift register function and draining the device battery [21,22]. On the other hand, altering system functionality may involve delivering an incorrect output or causing a program to malfunction. For example, a Trojan payload was designed to hinder data encryption by flipping a bit in the encrypted output upon activation [21, 22].

Payloads that ***damage circuitry*** involve identifying and exploiting a vulnerability in the system through which hardware or software can be damaged [26]. Damage can occur through actively hostile operations or passive modifications that cause the system to harm itself or degrade over time. [15] outlines techniques for dynamically adjusting a device's voltage and switching frequencies within its functional specifications but at levels that induce stress on the system. This stress can lead to performance degradation and accelerated hardware aging over time.

Payloads that ***leak information*** involve broadcasting sensitive information from the compromised device [26–28]. Trojans that leak information do not require a trigger since they typically do not affect the fundamental behavior of the circuit and will only be detected through power monitoring or some other form of side-channel analysis. A Trojan of this kind was proposed that utilizes voltage modulation on an unused pin to generate a radio frequency (RF) signal containing the encryption key, which can be intercepted and collected using an AM radio [21, 22] .

2.4 Trigger

The trigger of the HT is the event that activates the HT and delivers the payload. HT triggers bypass functional testing by relying on rare events, such as an atypical set of inputs or an unusual system state. Three common types of HT triggers are user-input by physical access, internal trigger by counter or event, and always-on [21, 22].

User-Input Trojans require the attacker to have physical access to the device in the field. [29] describes a "kill-switch" HT attack implemented into a microcontroller. The Trojan activates upon an attacker delivering an external signal, causing the Trojan to shut down the device. In [21,22], another Trojan is described, which leaks a private secret key whenever a specific text code is provided to the system. A strength of this type of trigger is that the attacker can precisely facilitate when the Trojan is activated. However, user-input attacks are often impractical if the device is in motion or resides in an unknown location.

Internal Trigger Trojans allow for a more autonomous attack, relying on the input scheme or state of the system to trigger the HT. Using this type of trigger, a HT can pass functionality testing by remaining dormant during testing and then triggering after it is in active use [30]. A widely used internal trigger mechanism for Trojan activation involves a time-based approach. The Trojan is programmed to activate only after a predetermined value on a counter or timer has been reached [31–33]. A time-based Trojan may leak sensitive information after a predetermined number of clock cycles or instruction executions. On the other hand, a state-based trigger may activate the Trojan when it detects a specific address on the first eight bits of an address bus [21, 22].

Always-On Trojans are permanently active and do not require a trigger. These types of HTs typically involve leaking or broadcasting sensitive data but may also include analog attacks, which involve changing physical parameters or components from the design specifications to cause faster device aging and degradation [26, 34]. Since the payload does not affect the system's primary function, the HT may not need a delayed trigger to ensure the Trojan passes testing. Always-On Trojans have been implemented by introducing additional components or modifying the physical properties of transmission lines to facilitate crosstalk, allowing the extraction of signals through covertly added transmission lines or external receivers [21, 22].

2.5 Previous HT Detection Methods

A variety of approaches have been developed to detect the insertion of hardware Trojans in electrical hardware, both during production testing and run-time. The approaches discussed in this section are Functional Testing, Structural Testing, Side-Channel Analysis (SCA), Run-Time Monitoring, Functional Obfuscation, and Structural Obfuscation.

Hardware Trojan can be detected through ***Functional Testing*** methods [35, 36], in which input schemes are applied to the system, and the observed outputs are compared with the expected outputs. This method aims to drive the system into all expected states in order to trigger the Trojan and reveal the attack at the output. While this method can be effective for simpler systems with few I/O ports, it has numerous shortcomings. First, as systems become more complex, the number of inputs and system states in a single device grows exponentially. As a result, exhaustive test procedures that check every input pattern are becoming impractical [37]. Secondly, HTs may perform unexpected functions that will not be detected in standard test schemes [29]. Thirdly, input testing may not reveal the Trojan if it is triggered by sequential events or activates under unexpected conditions [38].

HT detection by ***Structural Testing*** is addressed in [15, 36]. Structural testing involves examining the physical device after manufacturing to confirm the fabricated circuitry matches the intended design. However, without state-of-the-art inspection equipment, this is most easily accomplished through destructive reverse engineering. By removing the packaging and delayering the IC, the structure of the circuit can be observed to confirm it is Trojan-free. The disadvantage of this approach is that it is both time-consuming and requires sinking the cost of destroyed components [39]. Additionally, reverse engineering will likely fail to detect Trojans if they are only implemented in some of the manufactured chips.

This method is expanded upon through the use of ***Side-Channel Analysis (SCA)*** to detect unwanted circuitry [40, 41]. In this method, a "side-channel fingerprint" is developed by taking parametric measurements of a "golden model" chip, whose functionality and security have been confirmed by extensive I/O testing, destructive RE, or development in a trusted foundry [42]. These parametric measurements include power consumption, electromagnetic radiation, thermal emissions, or timing path delay. SCA detects Trojans in future chips by comparing the side-channel fingerprint of the device under test to that of the golden model. SCA is a promising detection technique, but it has its weaknesses. Like the previous detection methods, SCA suffers from scaling concerns as greater chip complexity leads to increased noise interference and process variation, making it difficult to confirm the presence of a HT [43, 44]. For this reason, SCA is most effective when the chip has low process variation and the Trojan consumes most of the chip's power and space resources. Conversely, it will begin to detect false positives when the chip has large amounts of process variation and the Trojan makes up a small portion of the circuit [45]. Multi-parameter side-channel analysis can help mitigate this problem by analyzing the process variation of multiple parameter measurements [46]. This approach helps eliminate the effects of process variation and reveals the parametric effects of the Trojan, making it easier to detect and address the attack.

Run-Time Monitoring techniques have been proposed which use machine learning (ML) to detect Trojans in real-time while the infected device is in operation [47, 48]. The ML algorithm can learn to recognize the system's usual performance, allowing it to detect anomalies caused by HT activation. The system can be designed to shut down in self-protection or reconfigure the system architecture to avoid the effects of the Trojan. ML models can also be employed during testing to automate and accelerate the collection and analysis of parametric measurements [15]. Research into ML Run-Time detection approaches is promising, but the techniques have significant overhead challenges. ML detection approaches demand a significant investment in software and hardware resources, including a larger dataset for ML algorithm training, increased system complexity, and implementation challenges [49].

In place of post-fabrication detection techniques, [50] proposes two front-end HT prevention techniques, ***Functional Obfuscation*** and ***Structural Obfuscation***. In the Functional Obfuscation method, an additional hardware layer is added to lock the functionality of the circuit until one or more digital keys are used to unlock it. Without the key, the device will not run, and the behavior cannot be observed, making it difficult for adversaries to study the circuit and extract IP or HT vulnerabilities [51]. On the other hand, Structural Obfuscation involves reorganizing the circuit's physical layout or adding arbitrary circuitry to make it difficult for an adversary to determine the circuit's behavior by visual inspection. Obscuring the circuit design makes it difficult for adversaries to reverse engineer the circuit and insert HTs [52]. For obfuscation to be viable, the circuit must be sufficiently complex, or it will be difficult to hide the circuit's functionality. The proposed obfuscation methods protect against reverse engineering methods without affecting the circuit's behavior. However, they present a design tradeoff that pits prevention efficacy against area, power, delay, and production overhead.

2.6 Security in Power Electronics

All of the previously discussed HT detection methods were studied and applied in computer technology applications. In this section, the security discussion will shift to the power electronics domain. In recent years, there has been increasing recognition of cybersecurity threats in power systems due to the growing use of IoT devices and remote control methods in power applications [53–57]. In addition to the system-level discussion of cybersecurity, there have been publications outlining board-level approaches to detecting HTs in PCB applications [58, 59]. However, there are limited publications addressing HT attack and detection methods in power applications at the IC/component level. This section will first cover the progress of power electronics security approaches at the system and board levels. Secondly, it will address the need for research into HT detection methods and IC-level security for power applications.

The discussion of security in the power electronics domain has pertained primarily to the system-level cybersecurity threats arising from network-driven control of power systems [60–63]. If an attacker can breach the network that provides remote-control capabilities for vehicles or industrial equipment, they can potentially gain unauthorized access to the controls. This could allow them to disable devices or even shut down the entire control system, presenting a significant risk to the safety and operation of the equipment [64]. In addition, the high volume of data traffic between IoT devices on a compromised network can make it easier for cybercriminals to engage in IP piitse information, further exacerbating the risks associated with a network breach. The high switching speeds and power consumption required in power systems applications make it crucial to quickly detect and respond to cyberattacks in order to prevent potential damages to the system [14].

Regarding hardware security in power electronics, the literature has only gone as deep as discussing the detection of HT attacks at the board level. For example, [58] suggests in-system measurement testing by which trace impedances and passive component values are confirmed in order to validate the integrity of the board design. This method may require the insertion of test points on the board to provide external access circuit nodes. It also requires significant space and cost overhead to accomplish the in-system test implementation. Alternatively, [59] proposes a method of detecting HTs on the PCB during in-field operation by monitoring the power consumption and using tuned thresholds to determine the presence of hardware Trojan activity. However, this detection approach assumes that the PCBs are functioning correctly with no faults. This is problematic due to the reliability problem in power electronics.

Reliability issues are prevalent in power electronics, as high-frequency switching and temperature cycling cause aging and stress on the physical components within the system. Over time, the thermal stress and power consumption lead to frequent failures in power devices [65]. Therefore, maintenance and component replacement are expected in the product lifecycle, and component failures do not raise suspicion of hardware attacks. As a result, HT attacks may be misdiagnosed as reliability faults, putting the reliability and security of the system at risk. For this reason, it is critical to advance research into power-related HT implementations and novel detection techniques that can identify HTs designed to evade traditional testing methods. Furthermore, as the advancement of IC technology drives their increasing implementation in power electronics [66, 67], thereby expanding the supply chain and introducing new vulnerabilities, the need for HT countermeasures grows even more vital.

Chapter 3

Methodology

3.1 Attacking the Gate Drive IC

In order to study hardware vulnerabilities in power systems, a typical power electronics circuit was chosen as a benchmark. The experimental circuit is a gate drive circuit with fault detection, specifically the ACPL-339J Dual-Output Gate Drive IC. The mechanics of this circuit were modeled in PSPICE ORCAD Capture circuit simulation software. The circuit was constructed in PSPICE and studied for vulnerabilities.

An overview of the gate drive architecture is shown in Fig. 3.1. The circuit drives a low-voltage PWM input to a high-voltage output. The ACPL-339J IC is equipped with short-circuit detection, which will trigger protective shut-down procedures within the device when a short-circuit fault is detected at the output. In the case of a short-circuit fault, the fault protection will electrically isolate the output from PWM logic, breaking the path from input to output. Additionally, the logic activates a transistor that provides a path from the output transistor's gate terminal to ground, effectively shutting off the device to prevent it from damage.

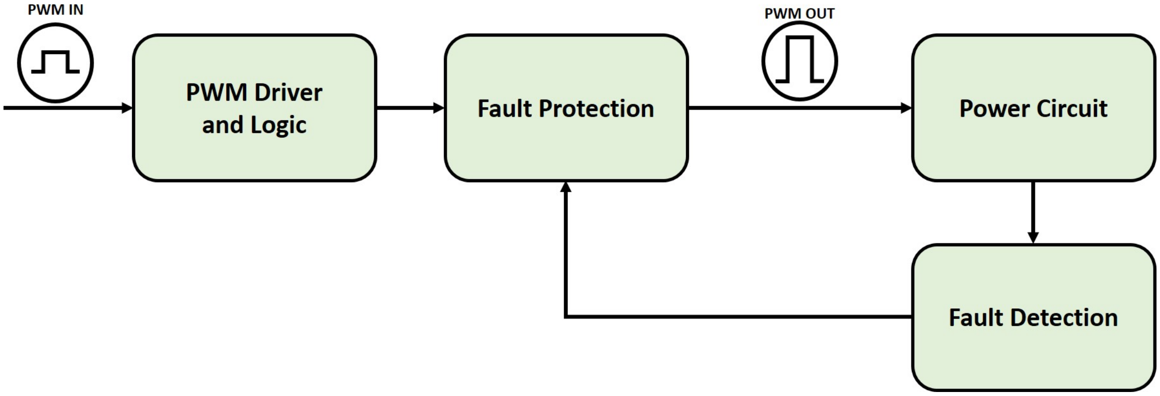


Figure 3.1: Basic architecture of the gate drive circuit

3.2 Fault Condition Trojan

The first goal of this research was to attack the fault detection circuitry and demonstrate how simple logic operations in a power electronics IC can pose security threats to the system. A hardware Trojan was proposed that could be implemented into the fault detection circuitry. This Trojan is referred to as the Fault Condition Trojan and will be discussed in Chapter 4.

3.3 HT Payload and Trigger Designs

After that, the research aim shifted to expanding the hardware security discussion into the power electronics domain by presenting new attacks that can be implemented into the gate drive circuit. Four payloads and five triggers were proposed that could be implemented into the gate drive circuitry. The proposed payloads and triggers were analyzed separately to emphasize the distinct characteristics and harmful potential of each attack mechanism.

The HT payloads and triggers proposed and investigated in this study were selected based on their expected effectiveness in the gate drive IC environment. Specifically, they exploit unique factors of the power electronics domain. For example, while payloads in computers typically exploit low-power digital logic, power electronics such as the gate drive IC have higher power levels and analog circuitry. These characteristics create new opportunities for payloads that can damage the circuit and surrounding systems. As a result, this study focuses on analyzing HT payloads that utilize analog characteristics of power electronics to cause damage to the circuitry in the gate drive

IC. Additionally, trigger mechanisms in computers are often concealed by complex circuitry and a myriad of input combinations. In contrast, the gate drive IC is a relatively simple and deterministic circuit comprised mostly of analog components. The pinout diagram for the gate drive IC is shown in Fig. 3.2 [68]. By inspection, it is easy to conclude that the device has limited I/O behavior from which to draw inspiration for effective hardware attacks. The IC's two primary functions are driving a PWM signal voltage from low-power inputs to high-power outputs and short-circuit protection. HT triggers were chosen to exploit these mechanisms and other factors, such as time and temperature. Chapters 5 and 6 will discuss the implementation efficacy and limitations of each proposed attack mechanism.

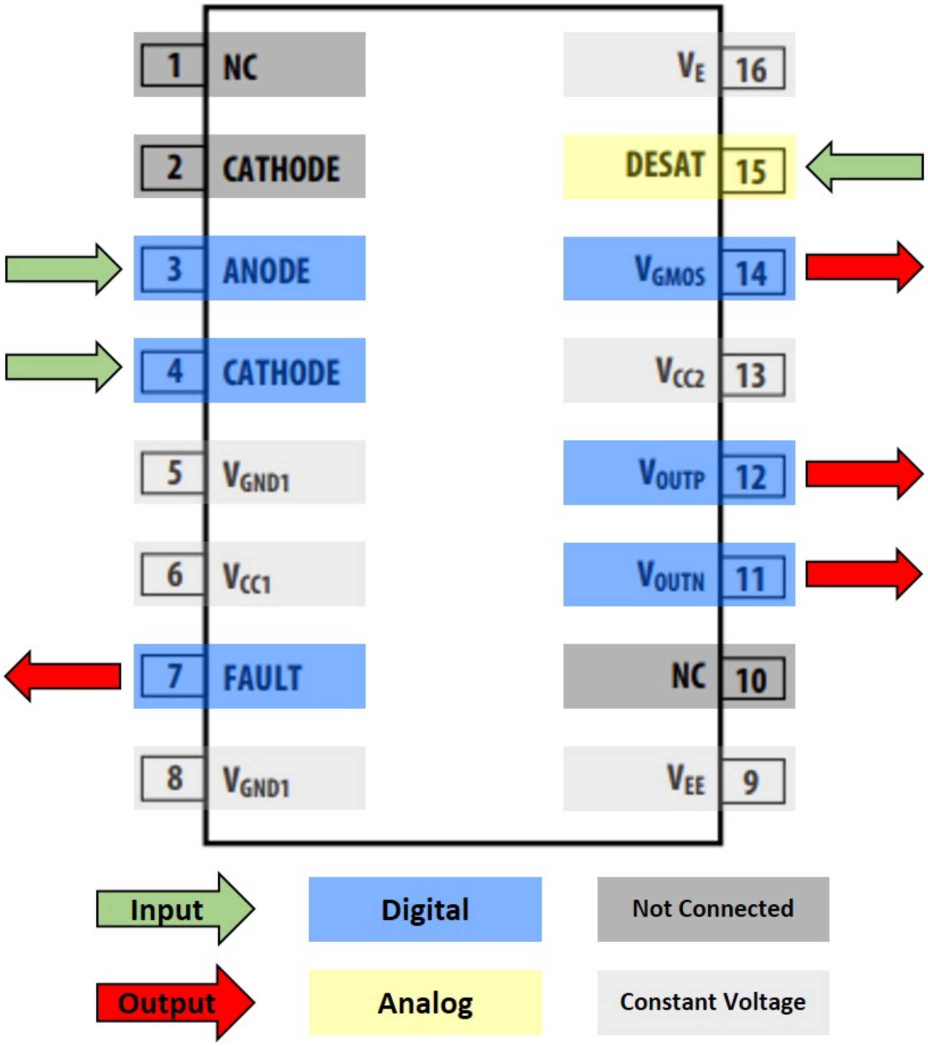


Figure 3.2: Pinout diagram of the ACPL-339J Gate Drive IC

Chapter 4

Fault Condition Trojan

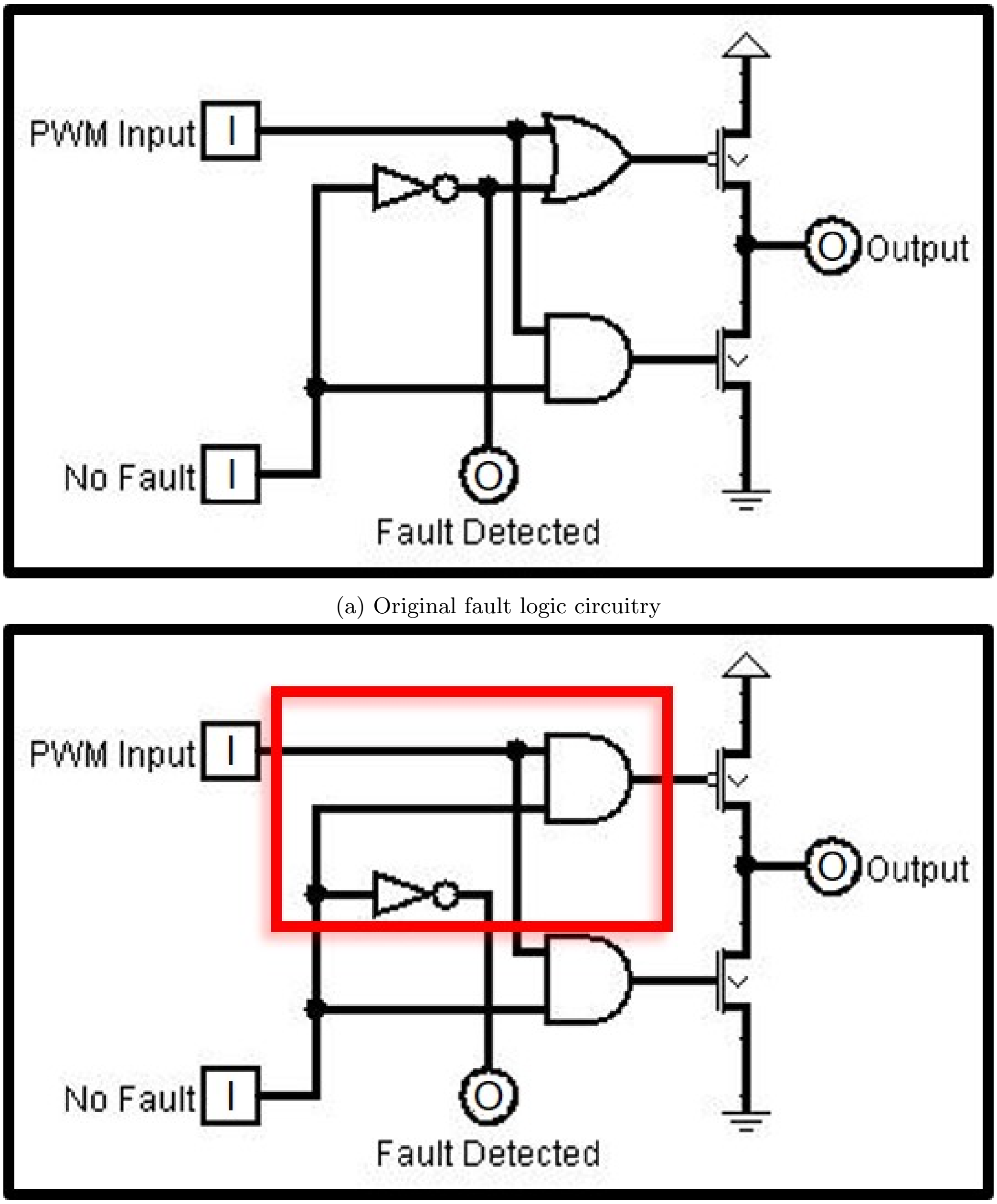
4.1 Exploiting the Fault Detection Logic

The Fault Condition Trojan was designed for the ACPL-339J gate drive IC and modeled in PSPICE simulation software. This Trojan demonstrates how an attacker can exploit simple logic implemented in a power electronics circuit. Specifically, it attacks the gate drive's fault logic, which is integrated with the system's desaturation (DESAT) short-circuit fault detection. The fault logic controls the transistors that propagate the input PWM signal to the output under normal conditions. When a short circuit fault is detected, the logic is designed to suspend vulnerable transistors so they do not sustain damage from conducting high currents.

The Fault Condition Trojan is implemented by swapping out one of the gates in the fault detection logic and modifying the gate connections, as shown in Fig. 4.1. The Trojan is triggered when a short circuit fault is detected at the output. Once triggered, the Trojan latches the output transistor in the active state, preventing the system's protective shut-down and forcing the transistor to conduct the short-circuit current.

4.2 Trojan Behavior

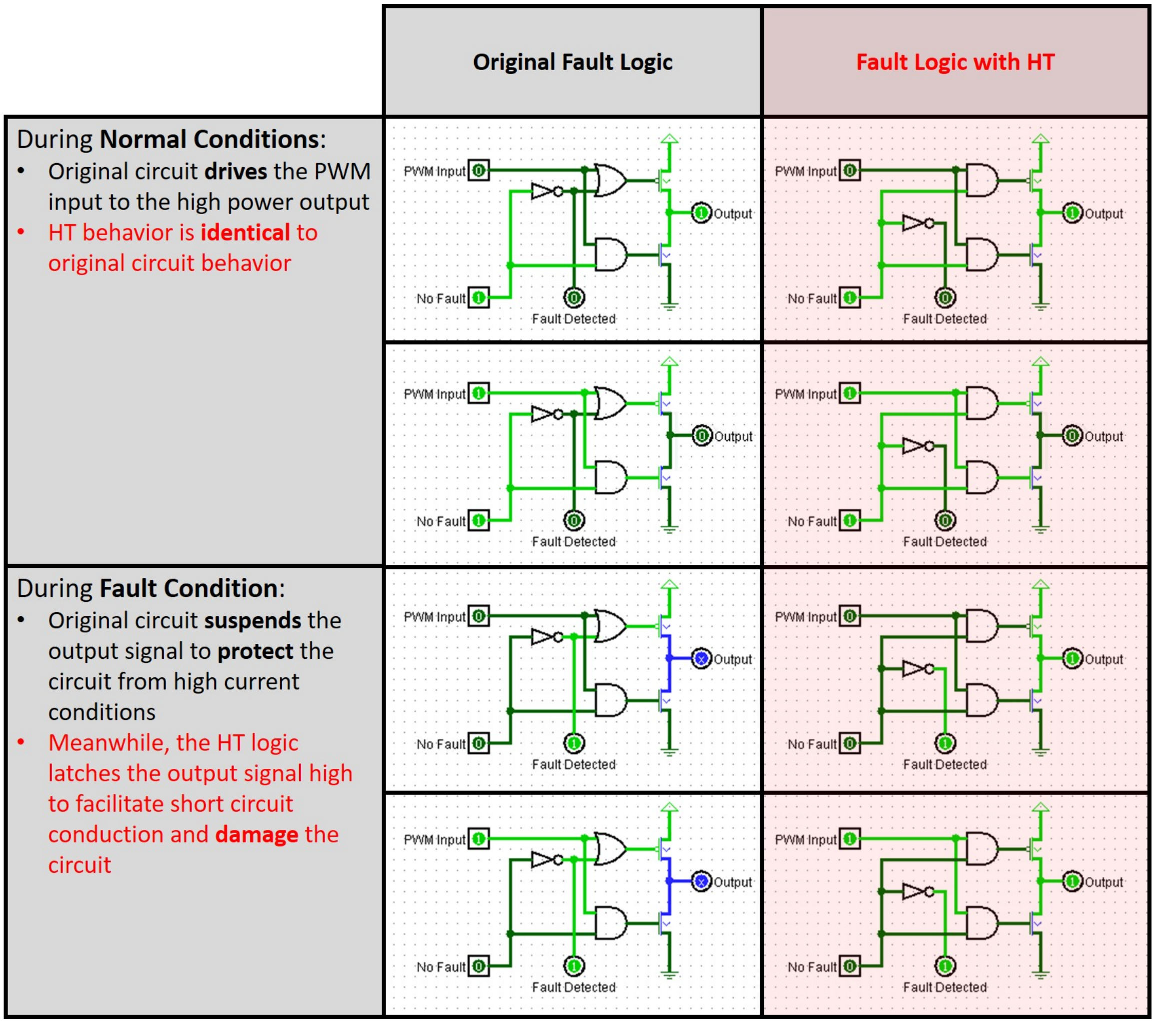
The circuit behavior before and after the insertion of the Trojan is shown in Fig. 4.2. Under normal operation, the circuit sends an inverted version of the input signal to the output to control the output power transistor, such that the voltage across the transistor mirrors the input voltage.



(a) Original fault logic circuitry

(b) Fault logic with Fault Condition Trojan inserted

Figure 4.1: The Fault Condition Trojan is implemented by slightly altering the fault logic. The red box shows where the OR gate was replaced with an AND gate, along with a couple of rewired connections



Original Fault Logic

Fault Logic with HT

During **Normal Conditions**:

- Original circuit **drives** the PWM input to the high power output
- HT behavior is **identical** to original circuit behavior

During **Fault Condition**:

- Original circuit **suspends** the output signal to **protect** the circuit from high current conditions
- Meanwhile, the HT logic latches the output signal high to facilitate short circuit conduction and **damage** the circuit

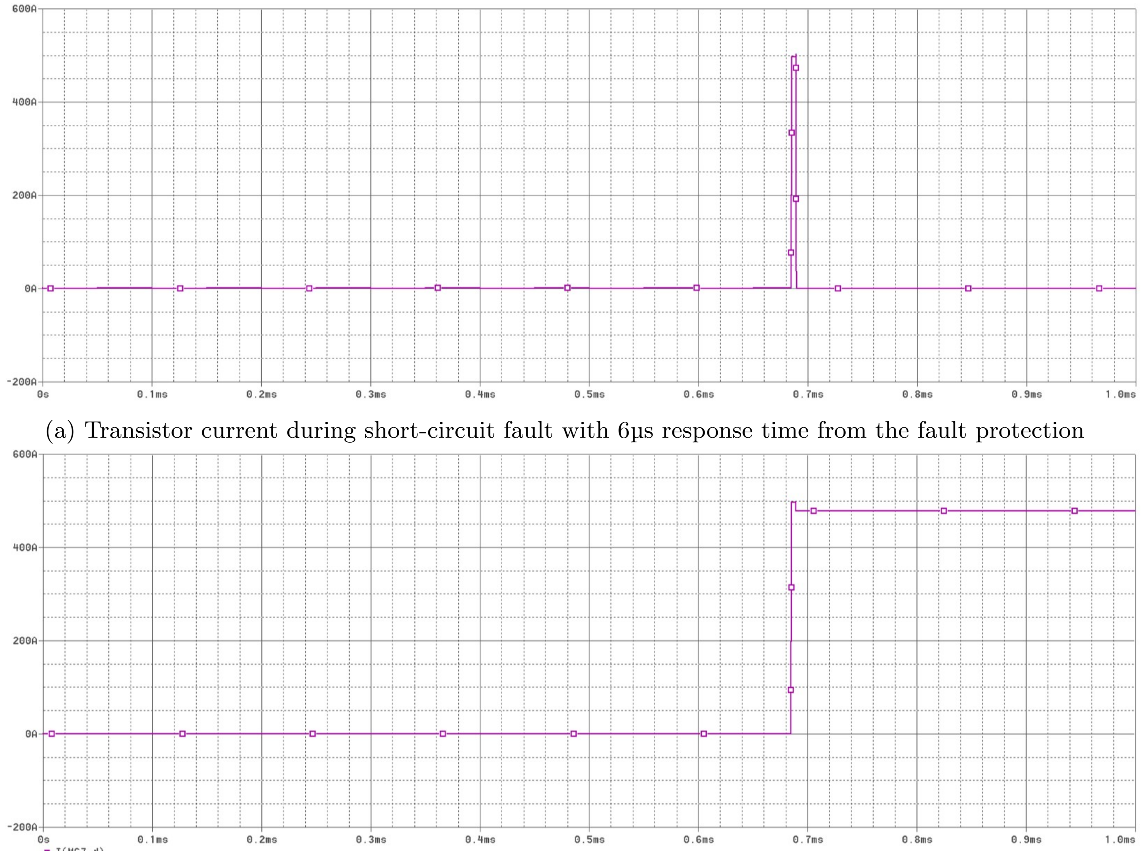
Figure 4.2: Behavioral comparison of the HT vs. the original circuit for every input/fault combination

When a fault is detected, the “No Fault” input voltage drops to zero, causing the logic to suspend the gate voltage of the output transistor. This shuts off the transistor, preventing it from conducting the short-circuit current and sustaining damage. The Trojan logic functions precisely the same under normal operation. When the “No Fault” signal is high, indicating that no fault has occurred, the Trojan logic sends an inverted version of the input signal to the output transistor. However, once a fault condition is detected, the Trojan behaves differently. Instead of suspending the output transistor, the Trojan ties the gate to a constant high voltage, forcing the transistor to conduct the short-circuit current.

4.3 Analysis

The Trojan-induced open-switch condition will damage the power transistor and likely cause issues with the circuitry downstream receiving a PWM signal that is constantly high [69]. Power switching devices, such as the TP65H035WS 650V GaN FET used at the output of the experimental gate drive circuit, can only withstand short-circuit currents for up to 13µs before sustaining damages [70]. Therefore, when this Trojan is activated during a short circuit fault, the output switching device will likely be destroyed. This demonstrates how an attacker could easily modify a circuit's logic, transforming its behavior from safeguarding against short circuit faults to exposing and damaging critical components and systems precisely when they are most vulnerable and in need of protection.

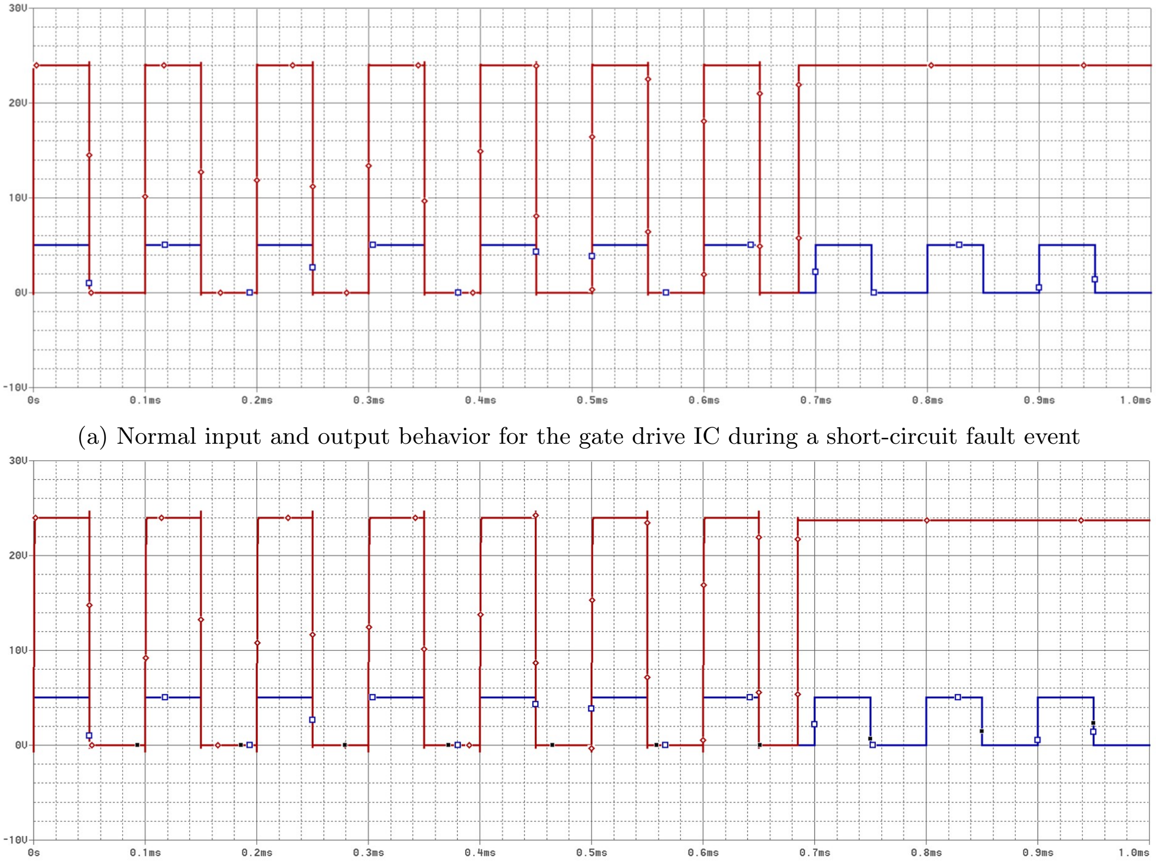
The transistor current during a short circuit fault is shown in Fig. 4.3a, which exhibits the response time of the gate drive's fault detection circuitry as it reacts to employ self-protective measures, shutting off the transistor in just under 7µs. On the other hand, Fig. 4.3b shows the transistor current for the Fault Condition Trojan, which prevents the gate drive's protective protocols and forces the transistor to bear the short-circuit current. Fig. 4.4a shows the input and output waveforms of the PWM signal during a fault-induced shutdown. The output voltage is latched to logic high after the short-circuit fault is detected at 685µs. This is because the switching transistor has been disabled by the protective circuitry, and the voltage difference across its source and drain indicates that current is not flowing. The I/O signals for the compromised circuit, shown in Fig. 4.4b, appear to behave similarly. However, after close inspection, it can be observed that the output voltage across the transistor experiences a slight drop after the fault occurs and the Trojan is triggered. This indicates that the high voltage drop observed across the transistor is not due to inactivity but is caused by its conduction of the short-circuit current, resulting in a significant portion of the voltage being dissipated through damaging levels of power consumption.



(a) Transistor current during short-circuit fault with 6µs response time from the fault protection

(b) Transistor current during short-circuit fault with extended short-circuit conduction due to the HT

Figure 4.3: Current spike through the output power MOFSET due to a short-circuit fault event at 685µs



(a) Normal input and output behavior for the gate drive IC during a short-circuit fault event

(b) Input and output behavior of the Fault Condition Trojan during a short-circuit fault event

Figure 4.4: The input and output voltages of the gate drive IC before and during a short-circuit fault event at 685µs

Chapter 5

Payload Designs

This chapter details the additional hardware Trojan payloads designed to attack the gate drive IC. The proposed payloads include Denial of Service, Circuit Damage, Internal Auxiliary System Attack, and Digital Communication Attack. At the end of the chapter, a system-level overview of the proposed payloads is illustrated in Fig. 5.1, and the discussion of results is summarized in Table 5.1.

5.1 Payload Type 1: Denial of Service

Description: This payload is delivered at the output of the circuit, known as a Denial of Service (DoS) attack. When triggered, a time-variant or normally active output is latched in an inactive state so that the behavior is disabled. This was implemented in the gate drive circuit by adjusting the PWM logic to disable the power transistor at the output. As a result, the output PWM signal becomes a constant low voltage, delivering no power to the output circuit.

Implementation Efficacy: This payload results in the system function or output being disabled, causing the system to shut down and require inspection and repair. If the DoS attack shuts down part of a grouped system, strain or damage could occur to the connected systems. A DoS attack has severe effects if it results in a system shutdown during crucial functionality, such as an aerial vehicle losing power mid-flight. A DoS attack is also relatively easy to implement since disabling any vital part of the system generally disables the output. DoS attacks are less likely to raise suspicion since faults are common in power electronics, meaning the fault is expected to be attributed to a reliability issue rather than malicious intent.

Limitations: The attack's severity depends on the vitality of the disabled function. A DoS attack may not result in significant damage or catastrophic results if it does not occur during crucial functionality. The attack may be attributed to a system fault and result in the failed device being replaced without causing substantial harm to the compromised system.

5.2 Payload Type 2: Circuit Damage

Description: This payload is delivered at the output of the circuit. When triggered, a time-variant output, such as a PWM, is tied in the active state. This is implemented in the gate drive circuit by altering the PWM logic to latch the output transistor in the active mode, delivering constant full power to the output power circuit.

Implementation Efficacy: Latching a circuit output to a high voltage will likely deliver damaging power levels to the devices and loads at the output. This is especially true in the case of a PWM circuit, where the power level is intentionally limited and moderated with switching methods. Payload Type 2 is very effective in causing harm to the target and may cause the system to be out of commission or need repair. The results can be catastrophic if this payload is delivered during a short circuit condition. The high power levels of the application make a circuit damage attack much more accessible to implement than in computer applications.

Limitations: Payload Type 2 requires careful design to properly exploit a system vulnerability such that physical damage is inflicted on the system. It is also a suspicious attack. Once the attack has occurred, the system will likely be closely inspected in root cause analysis. This means this type of attack will likely only be successful once, so its effects must be significant or it will not be very effective.

5.3 Payload Type 3: Internal Auxiliary System Attack

Description: This payload is delivered to an internal auxiliary system. The system can be activated or disabled depending on the desired attack. For example, a system may be falsely triggered when it is not supposed to, or it can be disabled so that it stops functioning or isn't functional when needed. Such systems can include internal monitoring, maintenance systems, or fault detection. In the gate drive circuit, this is implemented using logic to disconnect the digital input to the fault protection circuitry. When a fault is detected, the signal never makes it to the protection circuitry, resulting in the circuit failing to initiate protective methods and the output receiving the full effect of a short circuit fault.

Implementation Efficacy: If the fault protection circuitry is disabled, then the system cannot protect itself in the case of a short circuit fault. In our system, the fault protection circuitry disables the input logic and grounds the gate of the output power transistor. The result is that the transistor is shut off, ensuring that the high short-circuit current cannot pass through the transistor. An attack on this system allows the circuit to sustain severe damages during a short circuit fault. Payload Type 3 also has a lower detection probability at run-time, as it does not affect the primary function of the circuit. Therefore, it is less likely to be detected during primary functionality testing or after activation.

Limitations: Critical auxiliary systems are likely to be tested for correct functionality. To ensure this attack makes it through testing without being detected, it is necessary to carefully consider the vitality of the function under attack and choose trigger conditions.

5.4 Payload Type 4: Digital Communication Attack

Description: This payload is delivered to the internal digital communication system within the device. A digital communication line can be disabled, or a signal can be sent at an incorrect time. In the gate drive, this is implemented using simple logic to disable the IC's digital output pin related to the fault detection circuitry. The gate drive IC has a digital output pin that switches from low to high when a fault is detected. This Fault pin can be connected to a system controller to shut off power to the device at fault or manage the shutdown of related systems to protect the overall system from harm. By disabling this pin, the attack prevents communication with the controller and can result in protective protocols failing to initiate.

Implementation Efficacy: The Fault pin can be used to communicate with a control system in order to shut the system down so that the other portions of the system don't continue to run while the compromised system is malfunctioning. There are severe effects to disabling the subsequent communication systems of the fault detection circuitry. Attacking the Fault pin disables the device's communication of the fault to neighboring circuits, resulting in some parts of the converter running while the compromised device shuts down. Therefore, in the case of a fault, this attack causes damage to the greater system. An advantage of this attack is that it has lower detectability in functionality testing since it does not affect the main function of the circuit. It also may be less easily detected after triggering since it only affects subsequent functions.

Limitations: The fault pin attack requires a fault to occur. It also relies on the Fault pin being utilized for fault protection methods. The attack will be ineffective if the pin is not used for protective measures.

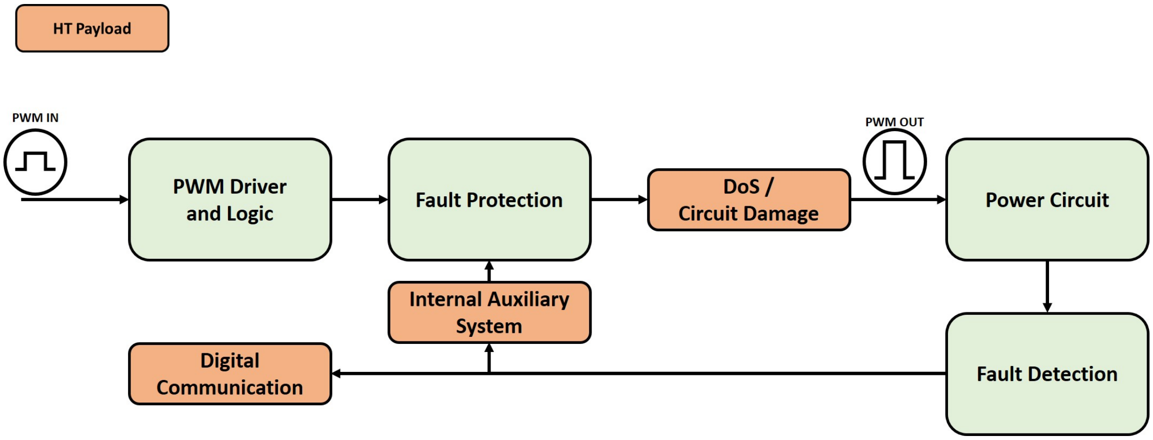


Figure 5.1: Proposed HT payloads for the gate drive IC

Payload	***Effect***	***Severity***	***Ease of Implementation***	***Stealthiness***
DoS	Disable output	Medium - High	High	Medium
Damage	Damage output switching transistor	High	Medium - High	Low
Auxiliary System	Cause auxiliary system to malfunction	Medium - High	High	Low - Medium
Digital Communication	Cause digital communication to malfunction	Low - Medium	High	High

Table 5.1: Summary of performance metrics for proposed HT payloads

Chapter 6

Trigger Designs

This chapter details the hardware Trojan triggers designed to attack the gate drive IC. The proposed triggers activate depending on the factors of time, system state, signal frequency, duty cycle, and temperature. At the end of the chapter, a system-level overview of the proposed triggers is illustrated in Fig. 6.1, and the discussion of results is summarized in Table 6.1.

6.1 Trigger Type 1: Time-based

Description: This trigger activates the Trojan after a certain amount of time. This time can be measured in real-time or run-time. In the case of real-time, the timer runs independently from the system and will activate the Trojan after a designated number of weeks or months. This design is best suited when the product deployment timeline is known, or there is a specific necessary time window for the attack. Alternatively, if the trigger is dependent on run-time, the timer is powered by the system or perpetuated by an internal clock. Since the timer will only run when the system is active, the trigger delay will depend on the time the system is actually running. This is a more optimal design if there is a long delay between product testing and deployment, or if it is necessary for the payload to be delivered during run-time.

A time-based trigger can be implemented with a counter, where the clock is connected to some binary signal in the circuit, such as a square wave, PWM signal, or digital signal. The trigger mechanism waits for a certain number of cycles and then activates the Trojan. The trigger delay is designed according to the switching frequency of the counter's input signal and the desired total trigger delay time. An independently powered clock is necessary for a real-time trigger delay, and standard testing and usage practices must be considered for a run-time trigger delay. In the gate drive, the counter clock is controlled by the PWM input for runtime measurement, but can be controlled by another internal voltage depending on the application. For example, the counter clock may be connected to the Fault pin such that it triggers the Trojan after a certain number of faults occur.

Implementation Efficacy: A real-time timer attack has very low detectability since it cannot be manually triggered. A run-time trigger would require many days or months of testing to detect the Trojan by activation. This trigger also has near-certain trigger probability since the attack is imminent given enough time.

Limitations: A real-time trigger requires an independent power source so that the timer can continue to run while the system is powered off, making it difficult to implement in smaller ICs.

6.2 Trigger Type 2: Fault Condition (State-based)

Description: A State-based trigger activates the Trojan when the system enters a particular state, such as a suspension state entered after the detection of a fault condition. Other system states may include low power mode, sleep, emergency lock-down, etc. A state-based Fault Condition attack exploits the short circuit fault detection circuitry. The implementation of this attack is discussed in more detail in the Fault Condition Trojan section above.

Implementation Efficacy: The gate drive's output transistor will sustain damages from the high current flowing through it. Additionally, the power circuit receiving the PWM control signal will receive full power delivery, potentially causing damage to electronic components and systems. The trigger probability of the fault condition Trojan is very high since faults occur commonly in dynamic power applications.

Limitations: A Fault Condition trigger will likely be detected in the product testing phase, as fault conditions are expected in power electronics systems, and fault detection systems will likely be tested for performance verification.

6.3 Trigger Type 3: Frequency

Description: This trigger activates the Trojan if the frequency of its input signal exceeds a particular threshold or enters a specific frequency range. This is implemented in the gate drive circuit by connecting the Trojan to the PWM input signal. Edge detection circuitry is used to detect the rising edge of the PWM signal and determine the signal frequency. The measured frequency is compared with the trigger condition frequency to activate the trigger when the trigger condition is met.

Implementation Efficacy: The Frequency Trigger can be tuned for a particular application. The detectability and trigger probability of a frequency Trojan will vary depending on the application and the design of the trigger. The further the designed trigger frequency is from the device's average functioning frequency, the less likely the trigger is to activate. The trigger likelihood of the Trojan is a matter of probability over the lifetime of the device.

Limitations: There is a tradeoff between the detectability and trigger probability of the frequency trigger. The more likely the trigger is to activate in the field, the more likely it will be detected in testing. Conversely, the stealthier the device is designed to be in the testing stage, the less likely it is to activate in the field to deliver the Trojan payload.

6.4 Trigger Type 4: Duty Cycle

Description: The duty cycle trigger activates the Trojan if the duty cycle of the input signal passes a particular threshold or enters a specific duty cycle range. This trigger is implemented in the gate drive IC using RC filtering to extract the duty cycle percentage value in reference to the source voltage. Comparators set the thresholds and trigger the Trojan when the designated duty cycle value or range is reached.

Implementation Efficacy: The implementation efficacy of the duty cycle trigger is very similar to that of the Frequency Trigger. Detectability and Trigger probability can be tuned by design and vary depending on the application.

Limitations: Similar to the Frequency Trigger, the designer of the duty cycle trigger must weigh the trade-off between a stealthy design with low detectability and an effective design with high trigger probability.

6.5 Trigger Type 5: Thermal

Description: The Thermal Trigger activates the Trojan if the ambient temperature passes a particular threshold or enters a specific temperature range. A thermal sensor hidden inside the device measures the temperature of the system, and comparison circuitry determines if the designed temperature threshold or range is reached. If so, the Trojan payload is delivered to the circuit.

Implementation Efficacy: Similar to the frequency and duty cycle triggers, the trigger probability depends on the application and the chosen temperature thresholds.

Limitations: A thermal trigger is very likely to be triggered in the testing phase because thorough temperature testing is a common practice to verify system functionality at temperatures beyond the specified temperature range.

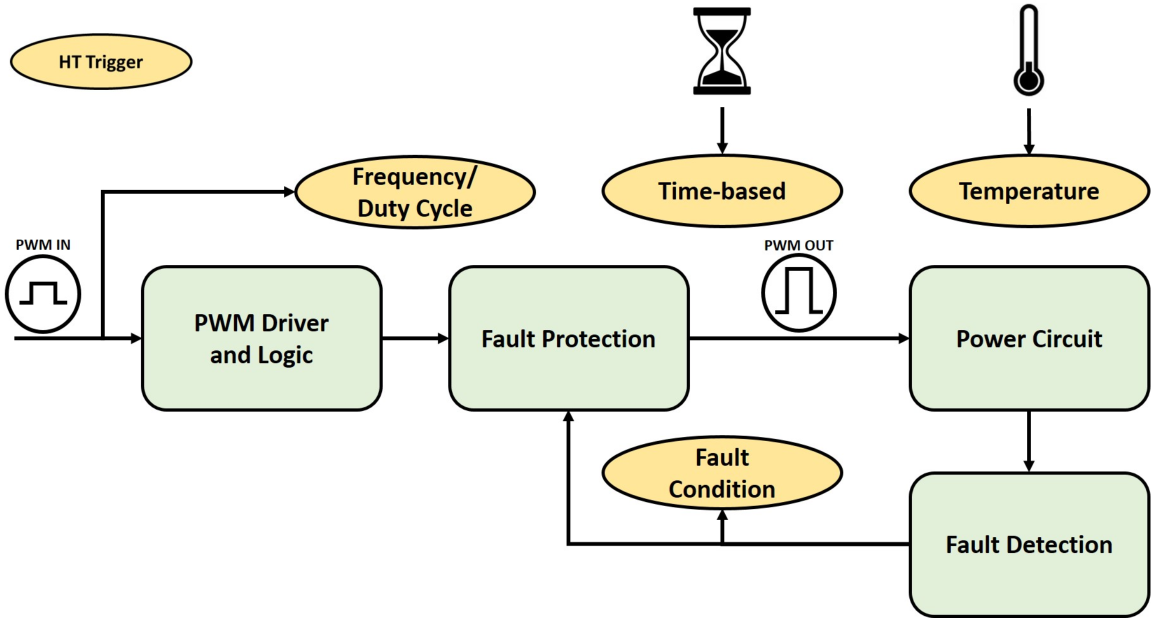


Figure 6.1: Proposed HT triggers for the gate drive IC

Trigger	***Trigger Condition***	***Trigger Probability***	***Ease of Implementation***	***Stealthiness***
Time	Timer reaches a predetermined value	Almost certain	Medium	High
Fault	Short-circuit fault is detected	Almost certain	High	Low
Frequency	Frequency of input signal enters specified range	Unlikely (tunable)	Medium	Medium - High
Duty Cycle	Duty cycle of input signal enters specified range	Unlikely (tunable)	Medium	Medium - High
Thermal	Temperature enters specified range	Unlikely (tunable)	Medium	Low

Table 6.1: Summary of performance metrics for proposed HT triggers

6.6 Trigger Combinations

In the previous sections, the efficacy and limitations of each attack mechanism were discussed in isolation. However, the performance of these triggers can be optimized when combined. By pairing the triggers together, the strengths can be optimized, and the weaknesses can be mitigated. It is important to consider these combinations, as they can make the Trojans much stealthier, and thus much more difficult to detect. We propose three significant trigger combinations in order to highlight the power of combining the triggers in a single application. The improved performance metrics of each trigger combination are covered in Table 6.2.

6.6.1 Timer + Frequency

Consider the combination of the Time-based Trigger with the Frequency Trigger. A design challenge of the Frequency Trigger is the trade-off between a stealthy design and a design that is likely to trigger. However, if it is combined with the Time-based Trigger is added, the combined trigger allows the attacker to guarantee that the Trojan will remain dormant until after the allotted time. This frees the attacker from the constraint of selecting a frequency or frequency range that is unlikely to be tested. Instead, the frequency can be chosen to optimize for the particular application. The Time-based Trigger can be combined with other triggers to create a time buffer before the other trigger becomes live and is ready to activate the Trojan. This can help the other triggers pass performance testing or buy time to build trust in the compromised system before deploying the payload.

6.6.2 Temperature + Fault Condition

Consider the implications of combining the Thermal Trigger with the Fault Condition Trigger. A shared weakness of these two triggers is that their trigger conditions are commonly tested in product testing schemes and, therefore, are likely to be detected during testing. Fault detection circuitry is likely to be tested to ensure the system can protect itself in the likely case of a fault. Similarly, the system will likely undergo thermal testing to verify temperature specifications and ensure proper functionality under extreme thermal conditions. However, if the two triggers are combined in series, such that both trigger conditions be met to activate the Trojan, the detection probability is drastically decreased. Consider the case where a high-temperature threshold is paired with a fault condition trigger. The likelihood that fault condition testing will be performed at extreme temperatures is low. It is more likely that fault testing and thermal testing will be performed independently of one another. Since the Trojan will pass fault condition testing at average temperatures, and a fault condition is unlikely to be detected or tested during thermal testing, the Trojan has a much higher chance of passing test procedures and making it out into the field.

6.6.3 Frequency + Duty Cycle

The Frequency Trigger and Duty Cycle Trigger may be combined to adjust their trigger probability. The trigger probability of each of these two triggers is tunable based on the chosen threshold or range. However, the Trojan's trigger probability can also be tuned by combining the two triggers, allowing for more reasonable threshold values. Then the trigger likelihood will have an additional input dimension and cannot be detected by a simple frequency or duty cycle sweep. Even at low probabilities, activation of the trigger is probable over a high amount of run time in the field.

Trigger Combination	***Trigger Probability***	***Ease of Implementation***	***Stealthiness***
Time + Frequency	Almost Certain	Medium	High
Thermal + Fault	Likely	High	High
Frequency + Duty Cycle	Likely	Medium	High

Table 6.2: Summary of optimized performance metrics achieved by combining trigger conditions

Chapter 7

Conclusions

7.1 Summary

The rapid growth of embedded systems in power electronics and the growing demand for cost-efficient solutions have led to the increased use of low-cost foundries in foreign countries, creating more opportunities for HT attacks. Despite extensive research on HTs in computer applications, there is a notable lack of consideration in the academic community regarding their potential threat in power electronics, resulting in a scarcity of related publications. This study ventured into the uncharted territory of HT research in power electronics, aiming to advance the improvement of functional testing schemes and the development of effective countermeasures against these attacks. By shedding light on this crucial area of concern, this study aimed to inspire further research and innovation in the field, ultimately leading to safer and more secure power electronics systems.

This research explored several HT attacks designed to target power electronics applications. A novel, functional hardware Trojan was implemented into a gate drive IC, which exploited the device's short-circuit fault protection logic in order to damage the output during a fault condition. Furthermore, several HT payloads and triggers were proposed which exploit the unique factors of the power electronics domain, such as high power delivery and analog circuitry. The proposed attack mechanisms are summarized in Fig. 7.1. The results demonstrated the potential of HT attacks in power electronics, highlighting the need for enhanced detection, protection, and prevention methods in power electronics applications.

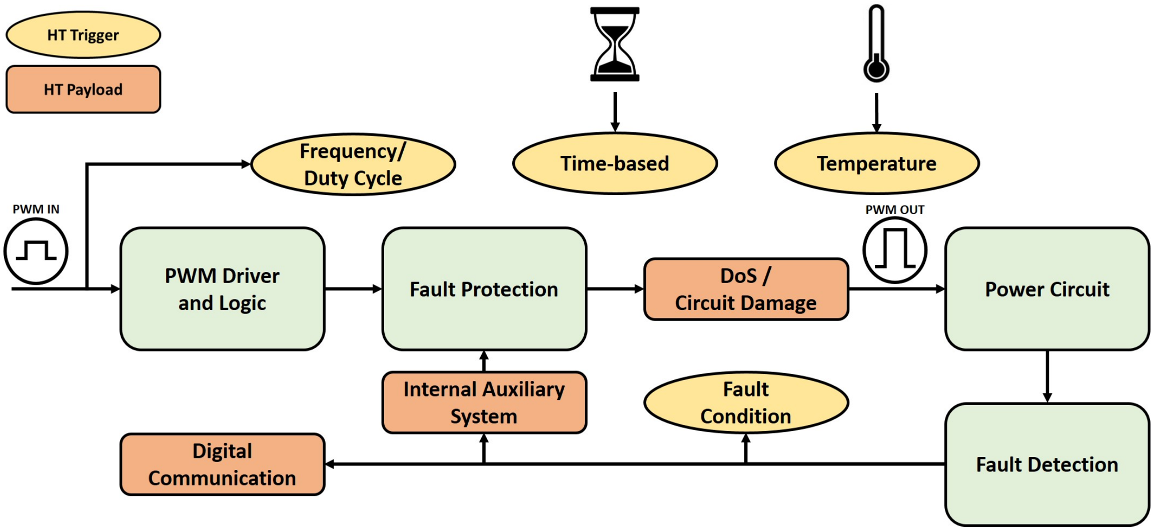


Figure 7.1: Summary of proposed HT payloads and triggers for the gate drive IC

7.2 Future Works

To build upon this research, further studies can be conducted to provide deeper insights into the design process of power electronics HT implementation by incorporating real-world benchmarks. This can help in understanding the impact of HT attacks on the performance and reliability of power systems. Additionally, by completing the HT design process through design, implementation, and testing, new insights can be acquired about attackers' approaches when employing HT attacks, which can help in developing more effective countermeasures. In particular, future research can focus on developing and evaluating detection and prevention schemes that mitigate the risks of HT attacks. This can involve the development of new algorithms and methodologies that can identify the presence of HTs in the system and analyze the system's behavior under HT attacks.

In summary, this study highlights the importance of addressing the threat of HT attacks in power electronics systems and provides a roadmap for future research in this area. With continued efforts to improve the design and security of power electronics systems, we can ensure their reliable and secure operation in critical applications.

Bibliography

[1] Yi Zhang, Xiaohan Shi, Hengxu Zhang, Yongji Cao, and Vladimir Terzija. Review on deep learning applications in frequency analysis and control of modern power system. *International Journal of Electrical Power & Energy Systems*, 136:107744, 2022.

[2] Haonan Xie, Meihui Jiang, Dongdong Zhang, Hui Hwang Goh, Tanveer Ahmad, Hui Liu, Tianhao Liu, Shuyao Wang, and Thomas Wu. Intellisense technology in the new power systems. *Renewable and Sustainable Energy Reviews*, 177:113229, 2023.

[3] Abhishek Kumar, Vikrant Singh, Saurabh Kumar, Shiva Pujan Jaiswal, and Vikas Singh Bhadoria. Iot enabled system to monitor and control greenhouse. *Materials Today: Proceedings*, 49:3137–3141, 2022. National Conference on Functional Materials: Emerging Technologies and Applications in Materials Science.

[4] Thomas A. Henzinger and Joseph Sifakis. The discipline of embedded systems design. *Computer*, 40(10):32–40, 2007.

[5] Keqiu Zeng, Saijun Mao, Gert Rietveld, Jelena Popovic, Hui Yu, Liguo Wang, Kun Liu, and Zhiding Zhou. High-precision control method for high-power mri gradient power amplifiers. *IEEE Transactions on Power Electronics*, 37(8):9035–9046, 2022.

[6] Boxuan Hu, Xiao-Lei Shi, Jin Zou, and Zhi-Gang Chen. Thermoelectrics for medical applications: Progress, challenges, and perspectives. *Chemical Engineering Journal*, 437:135268, 2022.

[7] Payam R. Badr, Behnaz Papari, Austin Robison, Christopher S. Edrington, Ahmed Abulebdah, Mustafa Alparslan Zehir, and Eman Hammad. Holistic performance benchmarking in power systems with distributed control under disruptive cyberattacks. In *2022 IEEE Transportation Electrification Conference & Expo (ITEC)*, pages 640–646, 2022.

[8] Yuchong Li and Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, 7:8176–8186, 2021.

[9] Yier Jin. Introduction to hardware security. *Electronics*, 4:763–784, 10 2015.

[10] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, 8(8):6222–6246, 2021.

[11] Md Sami Ul Islam Sami, Fahim Rahman, Farimah Farahmandi, Adam Cron, Mike Borza, and Mark Tehranipoor. Invited: End-to-end secure soc lifecycle management. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pages 1295–1298, 2021.

[12] Sophie Dupuis, Papa-Sidi Ba, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans. In *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, pages 49–54, 2014.

[13] Ujjwal Guin, Ziqi Zhou, and Adit Singh. A novel design-for-security (dfs) architecture to prevent unauthorized ic overproduction. In *2017 IEEE 35th VLSI Test Symposium (VTS)*, pages 1–6, 2017.

[14] Juan Carlos Balda, Alan Mantooth, Rick Blum, and Paolo Tenti. Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things. *IEEE Power Electronics Magazine*, 4(4):37–43, 2017.

[15] Wei Hu, Chip-Hong Chang, Anirban Sengupta, Swarup Bhunia, Ryan Kastner, and Hai Li. An overview of hardware security and trust: Threats, countermeasures, and design tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(6):1010–1038, 2021.

[16] Shivam Bhasin and Francesco Regazzoni. A survey on hardware trojan detection techniques. In *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2021–2024, 2015.

[17] Yier Jin and Yiorgos Makris. Hardware trojan detection using path delay fingerprint. *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 51–57, 2008.

[18] Joseph Clements and Yingjie Lao. Backdoor attacks on neural network operations. In *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1154–1158, 2018.

[19] Makoto Nagata, Takuji Miki, and Noriyuki Miura. Physical attack protection techniques for ic chip level hardware security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 30(1):5–14, 2022.

[20] Mary Asante, Gregory Epiphaniou, Carsten Maple, Haider Al-Khateeb, Mirko Bottarelli, and Kayhan Zrar Ghafoor. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, 2021.

[21] Hassan Salmani, Mohammad Tehranipoor, and Ramesh Karri. On design vulnerability analysis and trust benchmarks development. In *2013 IEEE 31st International Conference on Computer Design (ICCD)*, pages 471–474, 2013.

[22] Bicky Shakya, Tony He, Hassan Salmani, Domenic Forte, Swarup Bhunia, and Mark ehranipoor. Benchmarking of hardware trojans and maliciously affected circuits. In *Journal of Hardware and Systems Security (HaSS)*, pages 85–102, 2017.

[23] Travis Boraten and Avinash Kodi. Mitigation of hardware trojan based denial-of-service attack for secure nocs. *Journal of Parallel and Distributed Computing*, 111:24–38, 2018.

[24] Mehmet Bozdal, Maulana Randa, Mohammad Samie, and Ian Jennions. Hardware trojan enabled denial of service attack on can bus. *Procedia Manufacturing*, 16:47–52, 2018.

[25] Kohei Nozawa, Kento Hasegawa, Seira Hidano, Shinsaku Kiyomoto, Kazuo Hashimoto, and Nozomu Togawa. Adversarial examples for hardware-trojan detection at gate-level netlists. In *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5*, pages 341–359. Springer, 2020.

[26] Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno. A case study in hardware trojan design and implementation. *International Journal of Information Security*, 10:1–14, 2011.

[27] Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson. Trojan side-channels: Lightweight hardware trojans through side-channel engineering. In *Cryptographic Hardware and Embedded Systems-CHES 2009: 11th International Workshop Lausanne, Switzerland, September 6-9, 2009 Proceedings*, pages 382–395. Springer, 2009.

[28] Samaneh Ghandali, Thorben Moos, Amir Moradi, and Christof Paar. Side-channel hardware trojan for provably-secure sca-protected implementations. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 28(6):1435–1448, 2020.

[29] Trey Reece, Daniel B. Limbrick, Xiaowen Wang, Bradley T. Kiddie, and William H. Robinson. Stealth assessment of hardware trojans in a microcontroller. In *2012 IEEE 30th International Conference on Computer Design (ICCD)*, pages 139–142, 2012.

[30] He Li, Qiang Liu, and Jiliang Zhang. A survey of hardware trojan threat and defense. *Integration*, 55:426–437, 2016.

[31] Juan Carlos Martinez Santos and Yunsi Fei. Designing and implementing a malicious 8051 processor. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 63–66, 2012.

[32] Yinyuan Zhao, Xiaohang Wang, Yingtao Jiang, Liang Wang, Amit Kumar Singh, Letian Huang, and Mei Yang. An enhanced planned obsolescence attack by aging networks-on-chip. *Journal of Systems Architecture*, 117:102093, 2021.

[33] Sourav Das, Kanad Basu, Janardhan Rao Doppa, Partha Pratim Pande, Ramesh Karri, and Krishnendu Chakrabarty. Abetting planned obsolescence by aging 3d networks-on-chip. In *2018 Twelfth IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*, pages 1–8. IEEE, 2018.

[34] Mingfu Xue, Chongyan Gu, Weiqiang Liu, Shichao Yu, and Máire O'Neill. Ten years of hardware trojans: a survey from the attacker's perspective. *IET Computers & Digital Techniques*, 14(6):231–246, 2020.

[35] Julien Francq and Florian Frick. Introduction to hardware trojan detection methods. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 770–775, 2015.

[36] Rijoy Mukherjee, Sree Ranjani Rajendran, and Rajat Subhra Chakraborty. A comprehensive survey of physical and logic testing techniques for hardware trojan detection and prevention. *Journal of Cryptographic Engineering*, 12(4):495–522, 2022.

[37] Khoa D. Doan, Yingjie Lao, and Ping Li. Marksman backdoor: Backdoor attacks with arbitrary target class, 2022.

[38] Ayush Jain, Ziqi Zhou, and Ujjwal Guin. Survey of recent developments for hardware trojan detection. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE, 2021.

[39] Abdullah Nazma Nowroz, Kangqiao Hu, Farinaz Koushanfar, and Sherief Reda. Novel techniques for high-sensitivity hardware trojan detection using thermal and power maps. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(12):1792–1805, 2014.

[40] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. Trojan detection using ic fingerprinting. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 296–310, 2007.

[41] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers*, 27(1):10–25, 2010.

[42] Sina Faezi, Rozhin Yasaei, Anomadarshi Barua, and Mohammad Abdullah Al Faruque. Brain-inspired golden chip free hardware trojan detection. *IEEE Transactions on Information Forensics and Security*, 16:2697–2708, 2021.

[43] Daisuke Fujimoto, Makoto Nagata, Shivam Bhasin, and Jean-Luc Danger. A novel methodology for testing hardware security and trust exploiting on-chip power noise measurement. In *The 20th Asia and South Pacific Design Automation Conference*, pages 749–754, 2015.

[44] Hassan Salmani. Hardware trojan attacks and countermeasures. *Fundamentals of IP and SoC Security: Design, Verification, and Debug*, pages 247–276, 2017.

[45] Yier Jin, Nathan Kupp, and Yiorgos Makris. Experiences in hardware trojan design and implementation. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 50–57, 2009.

[46] Seetharam Narasimhan, Dongdong Du, Rajat Subhra Chakraborty, Somnath Paul, Francis G. Wolff, Christos A. Papachristou, Kaushik Roy, and Swarup Bhunia. Hardware trojan detection by multiple-parameter side-channel analysis. *IEEE Transactions on Computers*, 62(11):2183–2195, 2013.

[47] Amey Kulkarni, Youngok Pino, and Tinoosh Mohsenin. Svm-based real-time hardware trojan detection for many-core platform. In *2016 17th International Symposium on Quality Electronic Design (ISQED)*, pages 362–367, 2016.

[48] Joseph Clements and Yingjie Lao. Deephardmark: Towards watermarking neural network hardware. *Proceedings of the AAAI Conference on Artificial Intelligence*, 36(4):4450–4458, Jun. 2022.

[49] Zhixin Pan and Prabhat Mishra. A survey on hardware vulnerability analysis using machine learning. *IEEE Access*, 10, 2022.

[50] Yingjie Lao and Keshab K. Parhi. Obfuscating dsp circuits via high-level transformations. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 23(5):819–830, 2015.

[51] Surbhi Chhabra and Kusum Lata. Hardware obfuscation of aes ip core using combinational hardware trojan circuit for secure data transmission in iot applications. *Concurrency and Computation: Practice and Experience*, 34(21):e7058, 2022.

[52] NM Sivamangai and G Akashraj Nissi. Hardware obfuscation for ip protection of dsp applications. *Journal of Electronic Testing*, 38(1):9–20, 2022.

[53] Sudip K. Mazumder, Abhijit Kulkarni, Subham Sahoo, Frede Blaabjerg, H. Alan Mantooth, Juan Carlos Balda, Yue Zhao, Jorge A. Ramos-Ruiz, Prasad N. Enjeti, P. R. Kumar, Le Xie, Johan H. Enslin, Burak Ozpineci, Anuradha Annaswamy, Herbert L. Ginn, Feng Qiu, Jianzhe Liu, Besma Smida, Colin Ogilvie, Juan Ospina, Charalambos Konstantinou, Mark Stanovich, Karl Schoder, Michael Steurer, Tuyen Vu, Lina He, and Eduardo Pilo de la Fuente. A review of current research trends in power-electronic innovations in cyber–physical systems. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 9(5):5146–5163, 2021.

[54] Tehseen Mazhar, Hafiz Muhammad Irfan, Inayatul Haq, Inam Ullah, Madiha Ashraf, Tamara Al Shloul, Yazeed Yasin Ghadi, and Dalia H Elkamchouchi. Analysis of challenges and solutions of iot in smart grids using ai and machine learning techniques: A review. *Electronics*, 12(1):242, 2023.

[55] Meysam Gheisarnejad and Mohammad Hassan Khooban. Iot-based dc/dc deep learning power converter control: Real-time implementation. *IEEE Transactions on Power Electronics*, 35(12):13621–13630, 2020.

[56] Iordan Stoev, Snezhinka Zaharieva, and Adriana Borodzhieva. Internet of things (iot) application for temperature control in residential premises. In *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, pages 1–5. IEEE, 2022.

[57] R Raja Singh, Swapnil Banerjee, R Manikandan, Ketan Kotecha, V Indragandhi, and Subramaniyaswamy Vairavasundaram. Intelligent iot wind emulation system based on real-time data fetching approach. *IEEE Access*, 10:78253–78267, 2022.

[58] Matthew McGuire, Umit Ogras, and Sule Ozev. Pcb hardware trojans: Attack modes and detection strategies. In *2019 IEEE 37th VLSI Test Symposium (VTS)*, pages 1–6, 2019.

[59] Gor Piliposyan, Saqib Khursheed, and Daniele Rossi. Hardware trojan detection on a pcb through differential power monitoring. *IEEE Transactions on Emerging Topics in Computing*, 10(2):740–751, 2022.

[60] Yuanliang Li and Jun Yan. Cybersecurity of smart inverters in the smart grid: A survey. *IEEE Transactions on Power Electronics*, 38(2):2364–2383, 2023.

[61] Kirti Gupta, Subham Sahoo, Rabindra Mohanty, Bijaya Ketan Panigrahi, and Frede Blaabjerg. Distinguishing between cyber attacks and faults in power electronic systems–a non-invasive approach. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2022.

[62] Mohan Bharathidasan, V Indragandhi, Vishnu Suresh, Michał Jasiński, and Zbigniew Leonowicz. A review on electric vehicle: Technologies, energy trading, and cyber security. *Energy Reports*, 8:9662–9685, 2022.

[63] Mohammad Ghiasi, Taher Niknam, Zhanle Wang, Mehran Mehrandezh, Moslem Dehghani, and Noradin Ghadimi. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215:108975, 2023.

[64] Tiago Martins and Sérgio Vidal Garcia Oliveira. Cybersecurity in the power electronics. *IEEE Latin America Transactions*, 17(08):1300–1308, 2019.

[65] Dehao Qin, Gokhan Ozkan, Christopher Edrington, and Zheyu Zhang. Electrothermal management using in-situ junction temperature monitoring for enhanced reliability of sic-based power electronics. In *2021 IEEE Electric Ship Technologies Symposium (ESTS)*, pages 1–7, 2021.

[66] Yue Hao, Shuiying Xiang, Genquan Han, Jincheng Zhang, Xiao hua Ma, Zhangming Zhu, Xingxing Guo, Yahui Zhang, Yanan Han, Zi Wei Song, Y. Liu, Ling Yang, Hong Zhou, Jiangyi Shi, Wei Zhang, Min Xu, Weisheng Zhao, Biao Pan, Yangqi Huang, Qi Liu, Yimao Cai, Jian Zhu, Xinxiu Ou, Tiangui You, Huaqiang Wu, Bin Gao, Zhiyong Zhang, Guoping Guo, Yonghua Chen, Yong Liu, Xiangfei Chen, Chunlai Xue, Xingjun Wang, Lixia Zhao, Xihua Zou, Lian shan Yan, and Ming Li. Recent progress of integrated circuits and optoelectronic chips. *Science China Information Sciences*, 64:1–33, 2021.

[67] Tao Zhang, Jincheng Zhang, Hong Zhou, Yachao Zhang, Tangsheng Chen, Kai Zhang, Yi Wang, Kui Dang, Zhaoke Bian, Xiaoling Duan, Jing Ning, Shenglei Zhao, and Yue Hao. High-performance lateral gan schottky barrier diode on silicon substrate with low turn-on voltage of 0.31 v, high breakdown voltage of 2.65 kv and high-power figure-of-merit of 2.65 gw cm-2. *Applied Physics Express*, 12(4):046502, mar 2019.

[68] Avago Technologies. Acpl-339j dual-output gate drive optocoupler interface with integrated (vce) desat detection, fault and uvlo status feedback data sheet, April 2015.

[69] R.L. de Araujo Ribeiro, C.B. Jacobina, E.R.C. da Silva, and A.M.N. Lima. Fault detection of open-switch damage in voltage-fed pwm motor drive systems. *IEEE Transactions on Power Electronics*, 18(2):587–593, 2003.

[70] Nasser Badawi, Abdullah Eial Awwad, and Sibylle Dieckerhoff. Robustness in short-circuit mode: Benchmarking of 600v gan hemts with power si and sic mosfets. In *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*, pages 1–7, 2016.