1

Sneak Circuit and Power Electronic Systems

COPYRIGHTED MATERIAL

1.1 Reliability of Power Electronic Systems

Power electronics has already found an important place in modern technology, because it helps to meet the demands of energy, particularly in electrical form and efficient use of electricity. Application of power electronics is expanding exponentially in many areas, from computer power supply to industrial motor control, transportation, energy storage, electric power transmission, and distribution. Nowadays, over 70% of electrical loads are supplied through power electronic systems in the United States and Europe, and almost all electrical and electro-mechanical equipment contains power electronic circuits and/or systems. In the next 5 years, renewable energy systems (wind and solar, etc.) will show a sharp increase throughout the world, the needs of power electronic systems grow rapidly as a result. Therefore, the reliability of these systems should be a concern in its fundamental place in energy conversion and management.

A basic concept in reliability engineering is that part failure may cause system failure, and preventing part failure is effective in preventing system failure. Likewise, in power electronic systems, it is found that many system failures do result from component failures. The main factor affecting reliability at part level is the electrical and thermal stress of a component, such as device voltage, current, temperature, or temperature rise due to power dissipation, since the failure rate of the components will double with a 10°C increase in temperature. In order to achieve good reliability, system designers always apply effective reliability assurance techniques, for example, component derating, and thermal and electrical stress analysis, to manage the levels of component voltage, current, and power dissipation, and keep them well within rating limits.

However, not all system failures are caused by component failure. In some situations, no part has failed, yet the system performs improperly or initiates an

Sneak Circuits of Power Electronic Converters, First Edition. Bo Zhang and Dongyuan Qiu.
© 2015 John Wiley & Sons Singapore Pte Ltd. Published 2015 by John Wiley & Sons Singapore Pte Ltd.

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 2

undesired function. For example, an inadvertent launching of the Redstone rocket on 21 November 1961 resulted from an undetected design error in the electrical path. Such events may cause hazardous and even tragic consequences, which have been proven by many serious accidents in aerospace, navy, nuclear, and military industries in the last century.

A significant cause of such unintended events is named "sneak circuit," which is the unexpected electrical path or logic flow that can produce an undesired result under certain conditions [1]. Opposed to component failure, a sneak circuit happens without any physical failure in the system, causing an undesired effect in that system, although all parts are working within design specifications.

It is well established in reliability engineering that the more parts there are in a system, the more likely it is to fail. Complexity is considered as the main factor that causes sneak circuit, because it is difficult for the designers to have a complete view of the detailed interrelationship between components and functions in a complex system. As a consequence, sneak circuits may exist in a complex system, and produce undesired results or even prevent intended functions from occurring under certain conditions.

Nowadays, power electronic systems are being designed and manufactured with increased complexity to satisfy specific functions. Similar to other systems, the sneak circuit will affect the reliability of the power electronic system as well as part failure. Therefore, sneak circuit situations in different kinds of power electronic converters should be investigated and identified, which will have a positive impact on the reliability of the power electronic system.

1.2 Sneak Circuit

1.2.1 Definition of Sneak Circuit

A sneak circuit is a designed-in current path or signal flow within a system, which inhibits desired functions or causes unwanted functions to occur without a component having failed. Sneak circuits are not the result of component failures, electrostatic, electromagnetic or leakage factors, marginal parametric factors or slightly out-of-tolerance conditions. They are present but not always active conditions inadvertently designed into the system, coded into the software program, or triggered by human error [2].

Based on the definition of a sneak circuit, the sneak conditions may consist of hardware, software, operator actions, or any combinations of these elements. Thus, sneak circuits are a family of design problems, which includes four categories as follows [1]:

1. *Sneak path*:
   unexpected path along which current, energy, or logic sequence flows by an unintended route, resulting in unwanted functions or inhibiting a desired function.

2. *Sneak timing*:
   events occurring in an unexpected or conflicting hardware or logic sequence, which may cause or prevent activation or inhibition of a function at an unexpected time.
3. *Sneak indication*:
   ambiguous or false display of system operating status that may cause the system or operator to take an undesired action.
4. *Sneak label*:
   incorrect or imprecise nomenclature or instructions on system inputs, controls, displays, or buses, which may cause the operator to apply an incorrect stimulus to the system.

1.2.2 Examples of Sneak Circuits

Since the 1960s, many accidents in aerospace, navy, nuclear, military, and modern weapon systems, which caused hazardous and even tragic outcomes, have been found to be the result of sneak circuits. In addition, sneak circuits have also existed in household wiring and automobile electrical systems, which did not perform an intended function or initiated an undesired function. Some examples will be introduced in the following section to explain different types of sneak circuits.

1.2.2.1 Automobile Electrical System

Figure 1.1 shows an example of sneak path found in a mid-1960s automobile electrical circuit [1]. The circuitry design meets the electrical system specification, for example, when the ignition switch is on, power is supplied from the battery to the radio, and if the brake switch is closed, the brake lights receive power from the battery. Also, if the hazard switch (pedal) is on and the ignition switch is off, power will be supplied from the battery to the flasher module causing the brake lights to flash. In summary, all of the design intent had been satisfied.

However, a problem with this circuit design remains hidden. Assuming that the ignition switch is set to "off," the radio is switched to "on" and the hazard switch is enabled, if the brake pedal is depressed, power will be applied to turn the radio on with each flash of the brake lights. The cause of this unintended behavior, a sneak path, is highlighted in Figure 1.1. It is the brake switch (pedal) that provides a current path to the radio and places the radio parallel with the brake lights. In this case, the consequences of the sneak path are not severe; children left in the car by their parents could listen to the radio slowly draining the battery.

1.2.2.2 Household Wiring System

A popular household wiring system in Western European is shown in Figure 1.2a, which is a three-phase 127 V/50 Hz system with an approximately balanced load and

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 4

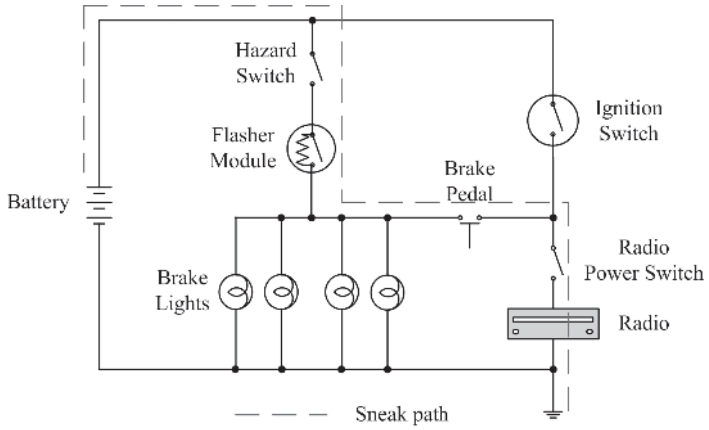


Figure 1.1 An automobile electrical system [1]

no neutral return wire. All devices or appliances are connected between lines and operate at 220 V [3]. If the fuse of phase B blows, a sneak path will appear as in Figure 1.2b, leaving devices in line A–B in series with those in line B–C across 220 V line A–C. Then the lamps on circuit A–B will dim if lamps or bath heater on circuit B–C is on and refrigerator operates erratically when the bath heater is on. Though all devices on circuit A–C work normally as before, phase B has no load, and phases A and C have overload, which will cause the distribution transformer to overheat.

1.2.2.3 A Sudden Acceleration Incident

In one kind of US police van, shown in Figure 1.3, the code 3 control switch activates a roof-mounted blue-light bar and causes brake lights and backup lights to pulse alternately at about 2.4 Hz. Diode (D) is used to prevent brake pedal switch from activating the blue-light bar via an alternating flasher relay. On 4 December 1998, an apparent police van shift lock failure combined with suspected misapplication of the accelerator rather than the brake resulted in sudden acceleration, the death of two pedestrians, and injury of nine [4]. It is found that closing code 3 control switch provides a pulsing path (sneak path) through flasher relay and diode D to disengage the shift lock, allowing the vehicle operator to shift into gear while applying the accelerator rather than the brake.

1.2.2.4 Redstone Rocket Launch Failure

Figure 1.4a shows the Mercury booster firing circuit of the Redstone rocket [3]. In order to satisfy the launching requirements, the motor is ignited by the on-board fire switch, annunciated by the ignition indicator light through an umbilicus, and the motor

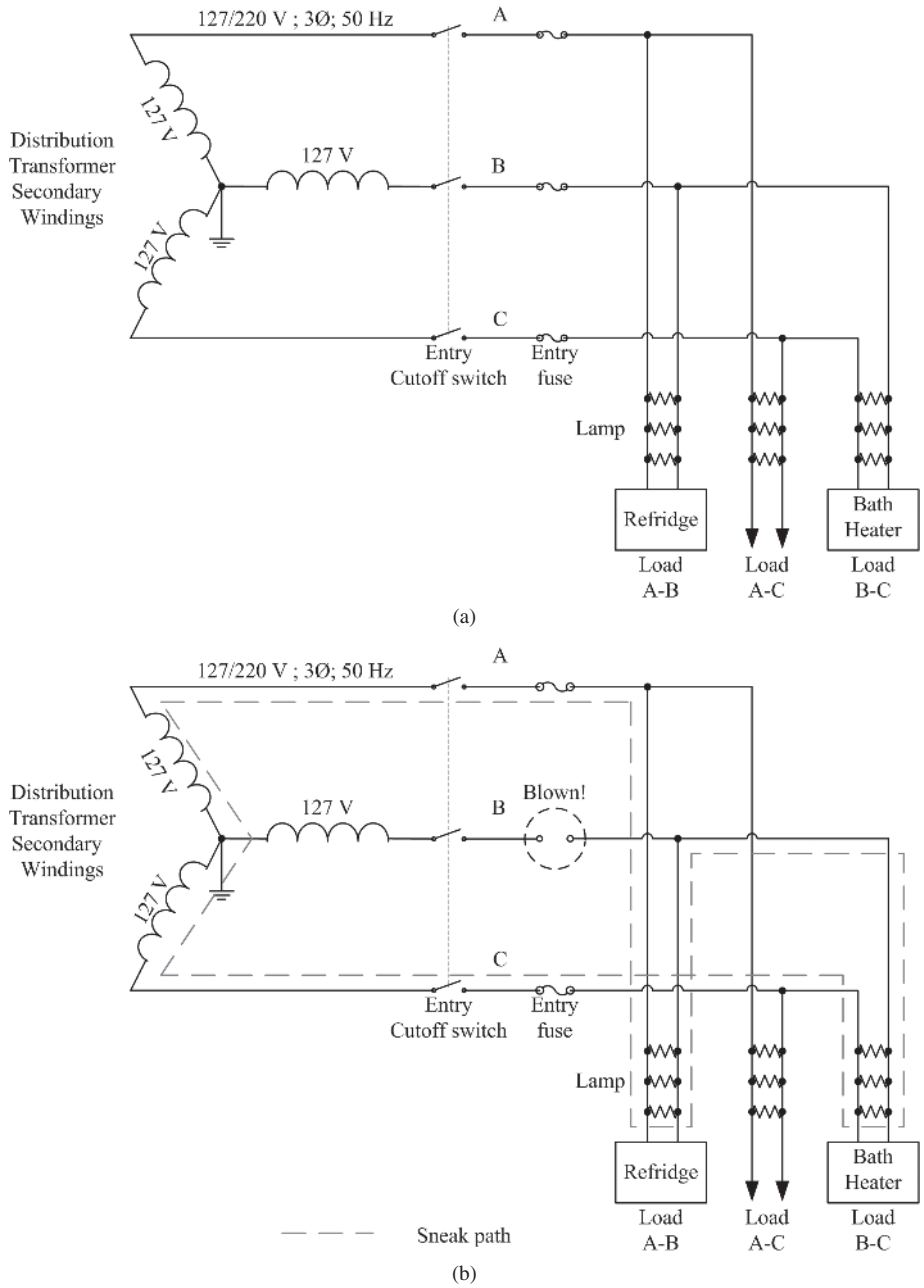


Figure 1.2 A household wiring system [3]: (a) normal operating state; and (b) state with broken fuse

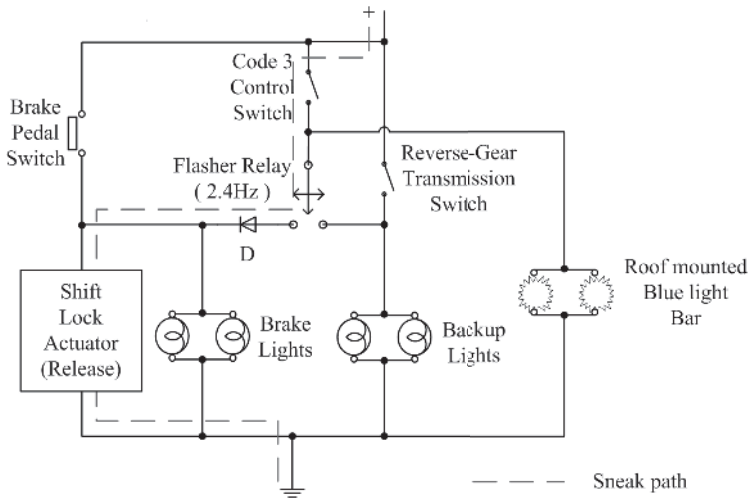


Figure 1.3 Part of control circuit in a police van [3]

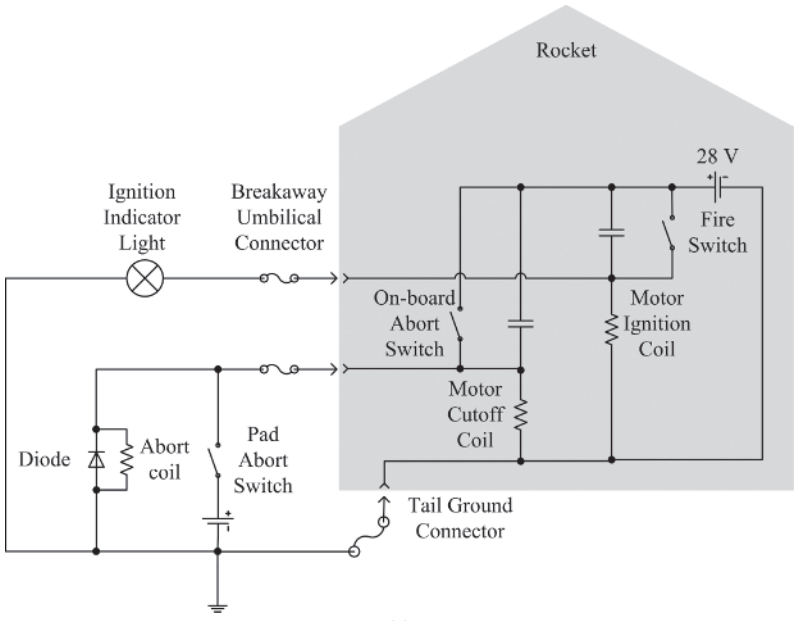
ignition coil latches to the on-board power supply (28 V). The on-board motor cutoff coil is energized by an on-board abort switch and latched to the on-board power supply. The abort prior to liftoff is enabled by the pad abort switch and the umbilical connector and tail ground connector are separate for liftoff breakaway. The Redstone rocket had launched successfully 60 times until 21 November 1961. On that day, the Redstone motor fired and began liftoff. After "flight" of a few inches, the motor cut off and the vehicle settled back on the pad. The Mercury capsule jettisoned and impacted 1200 ft away. The rocket was not allowed to be approached until the batteries had been drained down and liquid oxygen evaporated. Fortunately, damage was slight; booster and Mercury capsule were reused later.

This launch failure occurred due to the tail ground connector breaking away 29 ms prior to umbilicus separation, which meant that it was an incident caused by sneak timing. The tail ground connector was disconnected earlier than expected, leaving a current path, as shown in Figure 1.4b, for excitation of the motor cutoff coil through the ignition indicator light and suppressor diode, then the rocket landed back onto its launch pad after lifting just a few inches.

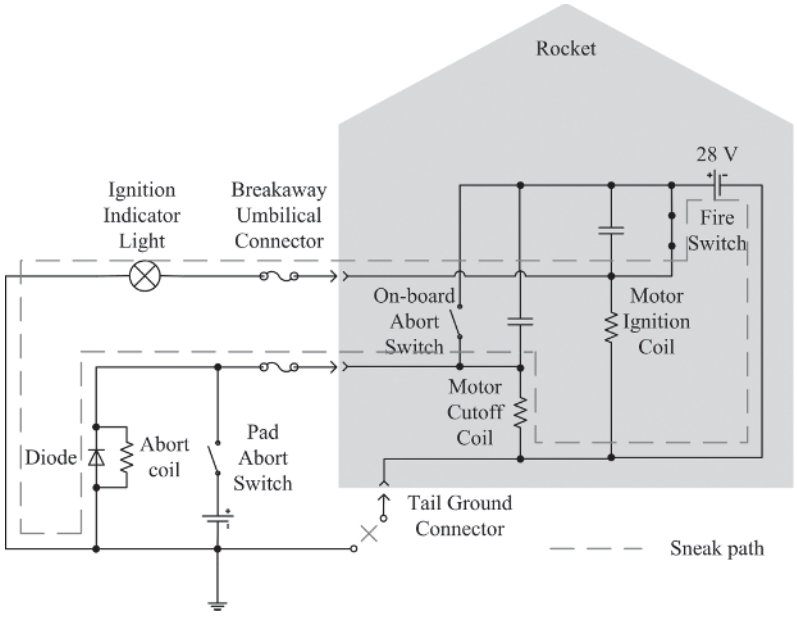
1.2.2.5 Three Mile Island Accident

On 28 March 1979, at the Three Mile Island (TIM) nuclear power plant in the USA, a relief valve solenoid excitation was interpreted as valve position, which resulted in destroying the TIM-2 reactor.

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 7



(a)



(b)

Figure 1.4 The Redstone booster firing circuit [3]; (a) schematics; and (b) sneak circuit path

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 8

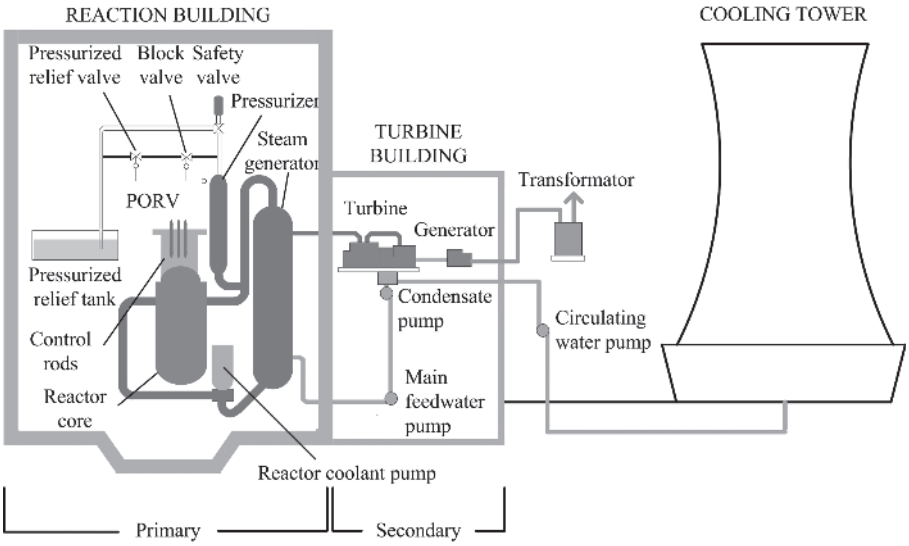


Figure 1.5 The #2 reactor of the Three Mile Island nuclear power plant [5]. (Source: Reproduced by permission of World Nuclear Association.)

The structure of the TIM-2 reactor is shown in Figure 1.5. The accident involved a relatively minor malfunction in the secondary cooling circuit, which caused the temperature in the primary coolant to rise. This in turn caused the reactor to shut down automatically. Within seconds of shutdown, the pilot-operated relief valve (PORV) on the reactor cooling system opened as intended, and at about 10 seconds later it should have closed. But it failed to close and the instrumentation did not indicate the valve's actual position. The operators believed that the relief valve had shut because instruments showed that a "close" signal was sent to the valve. As the valve remained open, so much of the primary coolant drained away that the residual decay heat in the reactor core was not removed and part of the core was melted in the #2 reactor. The core suffered severe damage as a result. Sneak indication has been proved to be the root cause of this accident [6].

1.2.2.6 Morgantown Rapid Transit System

The Morgantown Personal Rapid Transit (PRT) system is a one-of-a-kind people mover system in Morgantown, West Virginia, USA. This system entered operation in 1975 and has operated continually with 98% reliability for over 40 years. Even in such a highly reliable system, a sneak label problem was found [6]. As shown in Figure 1.6, a ganged switch S1, which connected both battery and critical system to the bus, was only labeled as "Battery Disconnect." When the operator disconnected the battery from the bus by turning off switch S1, the critical system was de-energized at the same time.

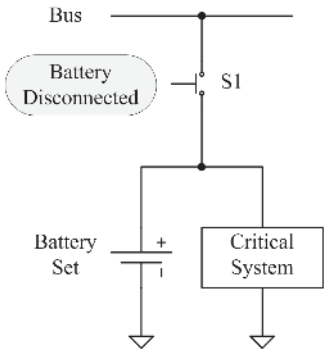


Figure 1.6 An example of a sneak label

1.2.3 Basic Causes of Sneak Circuit

As mentioned above, a sneak circuit is an unintended system path (e.g., wiring, tubing, software interfaces, operator actions, instrumentation, mechanical interlocks) or a latent condition (e.g., timing incompatibility), which is inadvertently introduced into the system. The principle causes of sneak circuits are system complexity, system changes, and user operations [1]:

1. *System complexity*:
   A complex hardware or software system normally requires numerous human interfaces between subsystems that may obscure intended functions or produce unintended functions. Under typical conditions of system design, it is difficult to ensure the understanding of subsystem interactions so completely that no possible variation in the flow of energy or logic, or in the actions of system operators, can fail to be noticed.
2. *System changes*:
   The effects of even minor wiring or software changes to subsystems may be undesired system operations. Because of subsystem interaction, a "fix" or corrective action that seems only minor and of local significance may produce changes in system functions that could not reasonably have been anticipated at the design stage.
3. *User operations*:
   A system that is relatively sneak-free can avoid desired functions, or generate undesired functions if the user employs improper operating methods or procedures. The cause could be simple human error on the part of the operator or inaccurate information supplied to that operator, for example, by a false indicator display or by an incorrectly labeled control.

With respect to all of these types of causes, complexity is the most common factor that will cause the sneak circuit. However, even a simple system may have sneak

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 10

circuits as well as the complex one. When systems become more complex, the probability of overlooking potentially undesirable conditions or creating sneak circuits is increased proportionately.

1.3 Sneak Circuit Analysis

1.3.1 Definition of Sneak Circuit Analysis

Sneak circuit analysis (SCA) is a generic term for a group of safety analytical techniques employed to methodically identify sneak circuits in systems, which can lead to anomalous behavior of the system [1, 7]. As described in the last section, a sneak circuit can be caused by inadvertent activation of signals, or the inhibition of signals when they are required to be activated. It can also be caused by the operator controlling the system inappropriately, or wrong information set by the system, such as incorrectly labeled controls or indicators. Therefore, SCA does not look specifically at the effects of component failures, but rather is concerned with the potential effects of latent path or logic flow that may exist in the hardware or software, in operator actions, or in some combination of these elements.

1.3.2 History of Sneak Circuit Analysis

In the past, sneak circuits were often discovered after the unintended effect had been observed in the actual system operation. Detection at this stage in the life cycle not only results in exposing the possibly serious operational effects of the sneak circuit, but may also require a significant expenditure of time and money to correct the problem and to retrofit the existing system. For these reasons, SCA should be developed to assist in the detection of sneak circuit early in system development.

Boeing were the first to develop SCA in the late 1960s, when they were commissioned by the National Aeronautics and Space Administration (NASA) to work on the Apollo and Skylab systems, in order to identify the designed-in conditions that could inhibit desired system functions or lead to catastrophic or otherwise financially costly incidents, such as the Redstone rocket launch failure. At that time, SCA was applied to purely electric circuits, which consisted mainly of discrete components such as relays, resistors, diodes, and vacuum tubes, and so on. Later, SCA was developed further by Boeing to cover computer software and complex designs that integrate hardware and software.

A company named Independent Design Analyses (IDA) has further developed a SCA technique since 1994, and used it to analyze Programmable Logic Devices (PLDs), Complex Programmable Logic Devices (CPLDs), and Application Specific Integrated Circuits (ASICs), and also applied it to software such as Sneak Software Analysis (SSWA). In 1997, the European Space Agency (ESA) published a procedure for implementing SCA, which specifically covered the application of SCA to both

hardware and software. It not only described the basic SCA procedure but also included a process which used the application of "clues" directly to components, to ensure that good design practices had been used throughout the system [8].

1.3.3 Methods of Sneak Circuit Analysis

SCA has been used extensively over the last 50 years as a safety analysis technique to verify the functionality of safety critical systems, and to remove any sneak paths that may have been inadvertently designed into the system. It has been used in various applications of differing complexity and make-up, from early electric circuits involving just discrete components, through analysis of software, to systems combining both software and complex integrated circuits. Among the currently available SCA methods, sneak path analysis, digital SCA, and software sneak path analysis have proved to be particularly useful [1].

1. *Sneak path analysis*:
   Sneak path analysis is a methodical evaluation of all possible electrical paths in a hardware system, which is used primarily to detect sneak circuits in electrical circuits.
   The sneak path analysis process consists of the following steps:
   (i) design elements, such as switches, diodes, and resistors, are converted into data inputs;
   (ii) computer runs path finding programs to identify all possible continuities for each operating mode of interest; and
   (iii) the program outputs are used to employ recognition of topological or functional patterns, with the aid of a rule base (i.e., sneak clues) derived from previous sneak circuit analyses.
2. *Digital sneak circuit analysis*:
   Digital SCA is performed on networks composed of digital functional modules, in which the elements of interest include logic gates, registers, flip-flops, and timers. Unlike sneak path analysis, which seeks to identify undesired paths in hard-wired circuits, digital SCA is concerned primarily with logic errors and inconsistencies, timing races, improper operating modes, and unintended switching patterns.
3. *Software sneak path analysis*:
   Software sneak path analysis examines computer program logic flows through an adaptation of the method used in sneak path analysis of hardware systems. Experience has shown that program flow diagrams containing sneak paths often exhibit similar characteristics.

SCA can be realized by the computer automatically, regardless of which SCA method is performed, and the requirement of collection, processing, and evaluation of detailed system design information is common [9]. The SCA results may be used

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 12

to support the activities of a variety of system functions, but its most important use is to aid in the improvement of design reliability prior to product manufacture and test.

1.3.4 Benefits of Sneak Circuit Analysis

SCA aims to identify the latent conditions within a system during the design process, thus SCA can benefit a system in the following ways [1].

1. *Detection of potentially serious system problems*:
   The major benefit of SCA results from the careful examination of a system for problems such as undesired and unintended current or logic paths, out-of-sequence events, false displays, and incorrect function labels. Identification of such anomalies is not the normal result of other analysis methods; generally, it is a unique output of SCA.
2. *Discovery of design oversights*:
   An SCA requires a detailed listing of components, connections, and timing sequences as well as current and signal flows, which gives a good chance of uncovering "design concerns" or possible design oversights. Examples of the types of concerns identified from an SCA, or from further investigation are part over-stressing, single failure point, unnecessary or unusual circuitry or components, lack of transient protection, and component misapplications.
3. *Discovery of documentation errors*:
   The detailed examination of system interfaces and circuitry required by SCA has, in many cases, uncovered drawing and documentation errors that might otherwise have escaped notice until a later stage of the development process.
4. *Reduction in system-change costs*:
   SCA is an analysis tool that can be used for hardware and software systems to identify latent paths, which will cause unwanted functions or inhibit desired functions, assuming all components and codes are functioning properly. Then a significant benefit of SCA is the prediction of these problems before they occur in test or operation. It is obvious that correction is more difficult and more time-consuming when physical changes to the system rather than modifications to drawings are required. Thus, the cost of modifications and redesign will be reduced if the problems are identified early in the development phase.
5. *Improvement to system reliability and safety*:
   The intent of the generally applied reliability and safety analysis is to identify system failures that will result from component failures. While such events certainly contribute a large share of a system's reliability problems, it is now clear that system failures can occur in the absence of part failures. Precluding such events through the use of SCA represents a real improvement in system reliability and safety.

6. *Reduction in testing and analysis requirements*:
   Dependence on extensive and time-consuming testing to detect sneak conditions adds to the cost of the development program and does not necessarily assure that such conditions will be identified. For example, a combination of events that can generate sneak circuits might not occur in a test routine; but a properly conducted SCA is specifically directed toward discovering such unusual conditions.
7. *Benefit to other analysis*:
   Applying SCA in the development phase can complement and facilitate other required analysis. As noted above in the discussion of design oversights, the detailed design review involved in SCA can identify misapplications, over-stressing, and similar problems. Equally important, some of the intermediate results of the SCA can materially assist in the performance of other reliability analysis.

Boeing has applied the SCA technology in over 200 projects for commercial, NASA, Department of Defense, and Boeing customers. In these projects, approaching 5000 sneak circuit problems have been identified and corrected, resulting in cost savings of hundreds of millions of dollars.

1.3.5 Relationship between Sneak Circuit Analysis and other Safety Techniques

The SCA technique differs from other systems analysis techniques in that it is based on identifying designed-in inadvertent modes of operation and is not based on the failed part. The relationship between SCA and other safety techniques are introduced briefly below [9–12].

Hazard and Operability analysis (HAZOP) is a safety technique conducted early in the developing cycle, which aims to identify potential safety hazards within a system caused by a parametric change in the flow of energy, whereas SCA looks for an undesired flow of energy in the form of a sneak path. HAZOP is undertaken using a different approach to SCA. It is performed by applying guide words, one at a time, that describe a non-idealistic behavior, to each of the flows (electrical signals) that are present in the system, in turn, to determine any adverse effects caused by that particular behavior. Guide words considered include both quantitative (e.g., less, more, none) and temporal aspects (e.g., early, late) applied to the flows in the system. SCA is a technique that complements HAZOP, since SCA looks for obscure interactions in the design of a system, whereas HAZOP investigates the effect of changes in the flow between functions in the system.

Functional Failure Analysis (FFA) is another safety technique, which considers the effects of a shortfall in the behavior of a function within the system, so it is performed

at functional level early in the design cycle, usually before the detailed design has been undertaken. FFA considers omission, commission, and invalid operation of the function to determine the possible effects and allow derived safety requirements to be generated to mitigate any potential safety impact. FFA would therefore be undertaken much earlier than SCA, since SCA is generally applied when a significant amount of design detail is available to evaluate, in order to identify sneak paths, as it is not possible to locate all sneak paths just by looking at the proposed functional hierarchy.

Failure Mode and Effect Analysis (FMEA) considers an aspect of system safety analysis that SCA does not cover, that is, it covers the consideration of failures of the system, through only one failure at a time. SCA is not concerned with failure mode analysis, so FMEA is a complementary technique that should be used in addition to SCA. There may be some overlap between these two techniques in what they highlight as problems, particularly from the design concern aspects output of SCA, some of which could lead to actual failures and hence will be caught by an FMEA.

In summary, SCA can be effectively blended with other safety techniques to identify design and fault related problems in a cost-effective manner. System reliability is improved by the combination of different safety techniques.

1.4 Power Electronic System and Sneak Circuit Analysis

SCA has been conducted on hardware and software to identify latent circuits and conditions that inhibit desired functions or cause undesired functions to occur without a component having failed. It has been used extensively over the last 50 years as a safety analysis technique to verify the functionality of safety critical systems and to remove many sneak paths that may have been inadvertently designed into the system. It has been used in various forms to target applications of differing complexity and make-up, from early electric circuits involving just discrete components, through analysis of software only projects, to systems combining both software and complex integrated circuits.

SCA is considered for application on high criticality systems, where undetected design flaws may cause catastrophic events, such as loss of life, critical system failure, or loss of mission. As the power electronic system plays an important role in electric power application, SCA should be carried out in the power electronic system to improve its reliability and safety. However, the power electronic system is one kind of switched-mode system in which the power electronic components are switching on/off under a fixed control sequence, in order to convert the input voltage or current to another form with higher efficiency.

As inductor and/or capacitor are often used as energy storage components in power electronic systems, there will be many electrical current paths in power electronic system, except those from source to ground. On the other hand, since the power electronic component, for example, Power Diode, Power MOSFET (metal oxide semiconductor field effect transistor), IGBT (insulated gate bipolar transistor), and so on, has parasitic

parameters, it is impossible to consider it as an ideal switch only with ON and OFF states, then the current flows in the power electronic system will be more complicated than those in the electrical system. Therefore, the presented SCA methods are not suitable for analyzing the sneak circuit problems in the power electronic system. The sneak circuit phenomena should be studied to investigate the SCA method for the power electronic system.

1.5 Arrangement of this Book

This book starts with an introductory chapter and moves on to power electronic converter topics on sneak circuit phenomena, methods for SCA and application guidelines. The book is organized into three parts, the first of which includes Chapters 2–5 on sneak circuit phenomena of some typical power electronic converters, such as resonant switched capacitor converters, basic non-isolated DC-DC converters, soft-switching converters, Z-source converters, and synchronous converters. The next part, including Chapters 6 and 7, presents three sneak circuit path analysis methods for power electronic converters based on the generalized matrix, adjacency matrix, and Boolean matrix respectively, and one sneak circuit mode analysis method based on mesh combination. The final part, comprising Chapters 8 and 9, focuses on the guidelines concerning elimination and application of sneak circuits in power electronic converters.

This book will help researchers and engineers, in the power electronics field and the related industries, to understand the fact that sneak circuits exist in power electronic systems objectively, and how to carry out SCA at the design stage to improve the reliability of power electronic systems.

References

[1] United States Navy (1986) *Sneak Circuit Analysis: A Means of Verifying Design Integrity*, University of Michigan Library.

[2] Buratti, D.L. and Godoy, S.G. (1982) Sneak Analysis Application Guidelines. Technical Report TR-82-179, Rome Air Development Center (RADC).

[3] Clemens, P.L. (2002) Sneak Circuit Analysis. Report, Jacobs Sverdrup, http://www.rdrop.com /users/larry/download/sneak%20wire.pdf

[4] Young, J.R. (1999) Report Documenting ODI's Investigation of a Sudden Acceleration Incident in Minneapolis, Minnesota on December 4, 1998, US DoT, National Highway Traffic Safety Administration.

[5] World Nuclear Association (2012) Three Mile Island Accident, http://www.world-nuclear.org/info /Safety-and-Security/Safety-of-Plants/Three-Mile-Island-accident/ (accessed 28 April 2014).

[6] Mason, J.F. (1979) An analysis of three mile Island. *IEEE Spectrum*, **16** (11).

[7] Rankin, J.P. (1973) Sneak-circuit analysis, *Nuclear Safety*, **14** (5), 461–469.

[8] Remnant, M. (2009) The application of sneak analysis to safety critical FPGAs. MSc Safety Critical Systems Engineering, The University of York.

[9] Walker, F.E. (1989) Sneak circuit analysis automation. Proceedings of Annual Reliability and Maintainability Symposium, pp. 502–506.

Trim Size: 170mm x 244mm Zhang c01.tex V3 - 09/08/2014 2:32 P.M. Page 16

[10] Savakoor, D.S., Bowles, J.B., and Bonnell, R.D. (1993) Combining sneak circuit analysis and failure modes and effects analysis. Proceedings of Annual Reliability and Maintainability Symposium, pp. 199–205.
[11] Jackson, T. (1986) Integration of sneak circuit analysis with FMEA. Proceedings of Annual Reliability and Maintainability Symposium, pp. 408–414.
[12] Wei, B.C. (1991) A unified approach to failure mode effects and criticality analysis (FMECA). Proceedings of Annual Reliability and Maintainability Symposium, pp. 260–271.