

меандрах были исследуемые алюминиевые пленки, а проводником служил слой V-Cu-Ni, полностью облуженный индиевым припоем. Ширина пленки алюминия составляла 200 мкм, площадь — 200 квадратов.

В результате проведенных исследований установлено, что кривые температурной зависимости относительного изменения сопротивления пленки имеют два характерных участка: в диапазоне температур от 4,2 К до 50 К — обусловленный остаточным сопротивлением, слабо зависящий от температуры и от 50 К до 300 К — прямо пропорционально зависящий от температуры. Этот результат можно объяснить тем, что перекрывающиеся металлические слои на алюминиевой подложке могут изменять поверхностный потенциал электронов проводимости на границе раздела, оказывая влияние на их число и подвижность вблизи поверхности. В зависимости от природы изменений, происходящих на границе раздела, сопротивление может или увеличиваться, или уменьшаться. Основным источником электрического сопротивления является рассеяние электронов на границах зерен, так как некоторая часть границ зерен ведет себя подобно свободным поверхностям. На величины электрического сопротивления проводников влияет также степень шероховатости поверхности, на которой сформирована исследуемая пленка.

МЕТОДИКА ПРОГНОЗИРОВАНИЯ НАДЁЖНОСТИ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ ПО ПОСТЕПЕННЫМ ОТКАЗАМ

Е.Н. Шнейдеров, И.А. Бурак, А.И. Бересневич

Методика позволяет применительно к конкретному экземпляру изделия электронной техники (ИЭТ) и заданной наработке t спрогнозировать значение его функционального параметра P и принять решение о надёжности экземпляра с учётом постепенного отказа для этой наработки. Соответствие рассматриваемого экземпляра требованию надёжности для заданной наработки t определяется сравнением прогнозного значения P с нормой, приведённой в технических условиях на ИЭТ, или со значением, указанным потребителем.

Индивидуальное прогнозирование применительно к испытываемому экземпляру выполняют методом имитационных воздействий, в основе которого лежит установление и использование статистических связей между изменениями параметров, вызываемыми, с одной стороны, имитационным воздействием, не приводящим к уменьшению рабочего ресурса ИЭТ, и, с другой стороны, — длительной наработкой (временем работы) ИЭТ [1]. Применение метода включает следующие этапы:

— экспериментальные исследования определённой выборки ИЭТ рассматриваемого типа вначале на воздействие имитационного фактора (здесь изменения параметров носят обратимый характер), а затем на длительную наработку (здесь изменения параметров носят необратимый характер);

— получение имитационной модели (функции пересчёта);

— определение ошибок прогнозирования;

— индивидуальное прогнозирование значения параметра P и, следовательно, надёжности (с учётом постепенного отказа) однотипных экземпляров, не принимавших участия в экспериментальных исследованиях.

Литература

1. Боровиков, С. М. Статистическое прогнозирование для отбраковки потенциально ненадёжных изделий электронной техники : монография / С. М. Боровиков. — М. : Новое знание, 2013. — 343 с.

ИСПЫТАНИЯ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ НА ДЛИТЕЛЬНУЮ НАРАБОТКУ

Е.Н. Шнейдеров, И.А. Бурак, А.И. Бересневич

Для решения задач оценки надёжности новых выборок изделий электронной техники (ИЭТ) методом индивидуального прогнозирования с использованием имитационных

воздействий и/или методом группового прогнозирования по моделям деградации функционального параметра необходим обучающий эксперимент. Этот эксперимент включает испытания выборки ИЭТ на длительную наработку с периодическим контролем их работоспособности и измерением рассматриваемого функционального параметра.

В качестве ИЭТ были выбраны биполярные транзисторы большой мощности типа КТ872А, интегральные транзисторы Дарлингтона типа КТ8225А, полевые транзисторы большой мощности типа КП723Г и интегральные стабилизаторы типа КР1180ЕН12А. Требуемое время испытаний с учётом наработки, приводимой в ТУ на ИЭТ, должно было составить 15...50 тысяч часов. Для сокращения времени использованы ускоренные испытания, проводимые по типовым методикам [1–3]. Основными видами форсированных воздействий при этих испытаниях были тепловая и электрическая нагрузки.

Результаты испытаний позволили разработать правила прогнозирования надёжности новых выборок ИЭТ, т.е. экземпляров, которые не принимали участия в испытаниях – обучающем эксперименте.

Литература

1. Боровиков С.М. Статистическое прогнозирование для отбраковки потенциально ненадёжных изделий электронной техники. М., 2013. 343 с.
2. Bipolar Power Transistor. Data Book 1998 / TEMIC Semiconductors. 1997. № 12. P. 35–42.
3. Robinson, L. E. Life expectancy in electronic components and the 10th rule / Robinson // Testing. 1998. № 1. P. 16.

ОБЗОР ТЕОРИЙ ДОКАЗАТЕЛЬСТВА ПРАВИЛЬНОСТИ ПРОГРАММ

В.А. Власенко

Традиционные методы анализа программного обеспечения в первую очередь связаны с доказательством правильности программ, ее верификацией. Данные методы не позволяют полностью выявить дефекты и установить корректность функционирования программы, поэтому существующие методы тестирования ограничены областью исследования и действуют только в рамках процесса проверки исследуемого или разрабатываемого программного обеспечения.

Эффективное тестирование сложных программных продуктов — это нетривиальный процесс, не сводящийся к следованию строгим и чётким процедурам и методологиям. Несмотря на данный факт, существуют методологии, описывающие основополагающие методики: идеи проведения доказательства частичной правильности программы, понятие слабейшего предусловия и прочие. Методы доказательства правильности программ принесли определенную пользу программированию. В некоторых случаях методы верификации могут применяться даже для обнаружения дефектов программного кода.

Как правило, исследователи отдельно выделяют средства для анализа безопасности программного обеспечения. Существуют два основных направления анализа безопасности приложений – статистического и динамического анализа исходных кодов (SAST, DAST, IAST).

Использование комплексного подхода, реализующего использование DAST, SAST и IAST на оптимальных этапах анализа, позволяет извлечь выгоду из всех подходов и позволит обеспечить глубокий анализ кода и API, а также провести практическую оценку безопасности программного обеспечения любой сложности.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ БИОМЕТРИЧЕСКИХ АУТЕНТИФИКАЦИОННЫХ СИСТЕМ

Г.А. Власова, А.М. Прудник

По мере того как биометрические компьютеризированные методы и устройства аутентификации становятся все более доступными, расширяется область их применения. Биометрические методы используются не только в наиболее защищаемых системах