Разработка плат по стандарту ISO 26262

Иван Селиванов (selivanov@megratec.ru)

ISO 26262 (ГОСТ Р ИСО 26262-1-2014) – большая и сложная спецификация, затрагивающая вопросы безопасности дорожных транспортных средств. Основное внимание в ней уделяется безопасности оператора транспортного средства, пассажира и обслуживающего персонала. ISO 26262 описывает весь жизненный цикл продукта, включая менеджмент, разработку, производство, эксплуатацию, обслуживание и вывод из эксплуатации. В данной статье рассмотрены аспекты спецификации, касающиеся этапов разработки и производства.

Ключевые аспекты стандарта ISO 26262

ISO 26262 разделяет риски возникновения опасности на 4 уровня полноты автомобильной безопасности (УПБА): A, B, C и D (по возрастанию уровня риска и требований функциональной безопасности). Рейтинги УПБА рассматриваются в контексте целей обеспечения защищённости автомобиля и основанных на них требований функциональной безопасности. Команда разработчиков преобразует последние в технические требования к системе безопасности (СБ), которые описывают механизацию и ожидаемые уровни производительности аппаратного и программного обеспечения. Технические требования к СБ становятся дополнительными функциональными требованиями, помимо обычных требований к проекту, связанных с безопасностью. Сопоставление всех указанных целей и требований – ключевая часть плана обеспечения безопасности продукта. Другая его часть – документирование механизмов безопасности, обеспечивающих предотвращение или обнаружение и смягчение отказов.

ISO 26262 определяет требуемые методологии проектирования и показатели надёжности в зависимости от УПБА. Средства разработки обязаны обеспечивать отслеживание требований и необходимый уровень анализа, производительности и целостности в соответствии с заданным УПБА для соответствующей части проекта и процесса проектирования.

Проект электронной части автомобиля содержит в среднем от 2 до 7 целей безопасности, каждой из которых соответствует от 1 до 5 требований функциональной безопасности. Команда разработчиков выдвигает одно или несколько технических требований к СБ для реализации каждого функционального требования безопасности. Обычно множество частей проекта влияют на несколько технических требований к системе безопасности с разными УПБА. Для более строгих УПБА (B, C и D) требуется более полный анализ, включающий расчёт вероятности случайного отказа оборудования для каждой цели безопасности. Выполнение этих сложных требований к анализу становится проще благодаря дополнительной документации и атрибутам, задаваемым на уровне схемы, и должным образом документируемым при разработке топологии печатной платы.

Наиболее вероятные нарушения требований безопасности автомобиля, связанные с печатными платами

Электронные системы автомобиля очень разнообразны, и так же разнообразны цели обеспечения безопасности, связанные с ними. Современные электронные системы автомобиля с высоким (УПБА C и D) уровнем функциональных требований безопасности – это:

- беспилотное управление;
- электроусилитель руля;
- адаптивный круиз-контроль;
- система мониторинга усталости водителя (система контроля и удержания в полосе, система обнаружения препятствий);
- гибридный/электрический привод (инверторы для управления электромотором, управление АКБ, заряд батареи / преобразователи постоянного тока);
- управление приводом (системы управления двигателем/трансмиссией/КПП/дифференциалом).

Существует также огромное количество систем с УПБА A и B, таких как датчик дождя / управление стеклоочистителем, управление климатом (оттаивание), контроллеры генератора и распределения питания.

С учётом вариативности их специфики от продукта к продукту цели обеспечения безопасности обычно подпадают под одну из следующих категорий:

- потеря/неправильная работа рулевого управления;
- избыточный/недостаточный крутящий момент на колёсах (движение, регенерация и торможение);
- непредусмотренный крутящий момент на колёсах;
- риски, связанные с высоким напряжением / большим током;
- потеря/неправильный анализ данных с сенсоров;
- полная/частичная потеря функционала;
- потеря/неправильная работа обратной связи с водителем;
- потеря/неправильное взаимодействие с контроллером.

Параметры среды разработки печатных плат, критичные для функциональной безопасности

Для того чтобы убедиться, что требования безопасности не нарушены, необходим соответствующий функционал среды разработки. Его смысл состоит в том, чтобы проектный замысел был аккуратно и надёжно зафиксирован в физическом проекте вместе со ссылками на документацию, содержащую соответствующие функциональные требования. Среда разработки печатных плат должна обеспечивать следующие концепции целостности проекта:

1. Целостность списка цепей, получаемого из схемы:

- схема представляет собой детализированный проектный замысел и является основным документом, описывающим проектный замысел;
- список электрических цепей определяет трассировку печатной платы;
- список электрических цепей определяет работу инструментов моделиро-

вания электрических цепей для верификации проекта.

2. Целостность перечня элементов, получаемого на основе схемы: перечень должен корректно представлять электрические компоненты, используемые в схеме.
3. Целостность данных при генерации топологии (списка физических цепей) на основе списка электрических цепей: топология печатной платы должна отражать список электрических цепей, чтобы удостовериться в корректной имплементации цепей.
4. Корректность воплощения электрических требований на печатной плате: требования к зазорам на основе импеданса, длинам цепей на основе задержек и ширине дорожек на основе падения напряжения должны быть корректно интерпретированы и реализованы.
5. Целостность механических ограничений (зазоры и порядок слоёв):

- физические расстояния между трассами и компонентами должны быть правильно интерпретированы и реализованы для выполнения требований к зазорам и утечкам (во избежание скрытых сбоев и электрических опасностей);
- физические расстояния между компонентами должны быть правильно интерпретированы и реализованы для правильной сборки (во избежание скрытых повреждений, связанных со сборкой);
- данные по слоям должны быть правильно интерпретированы и реализованы, чтобы избежать нарушения вертикальных зазоров и утечек.

6. Целостность данных, передаваемых на изготовление: файлы ODB++, Gerber должны содержать точные данные для изготовления, сборки и тестирования печатной платы.

Краткие требования к документированию функциональной безопасности

Конечная цель – разработать и должным образом задокументировать продукт, соответствующий всем требованиям. Стандарт ISO 26262 сосредоточен на требованиях, касающихся безопасности, которые должны быть описаны в виде технических требований к СБ со ссылкой на соответствующие требования функциональной безопасности и представлены заказчику в форме, позволяющей продемонстрировать, что транспортное средство соответствует поставленным целям.

Каждому требованию функциональной безопасности соответствует рейтинг УПБА, который должен учитываться в процессе проектирования и анализа. Требования функциональной безопасности задаются на уровне системы (продукта). План безопасности разрабатывается параллельно с механизацией системы. Он определяет технические требования к СБ для выполнения функциональных требований безопасности для текущего уровня механизации. Технические требования к безопасности добавляются к общим функциональным требованиям системы. Чертёж механизации системы – критически важный этап в процессе документирования. Он должен чётко определять интерфейсы связи между системами автомобиля, а также охватывать технические требования безопасности, ассоциированные с программной и аппаратной механизацией.

Ключевая концепция состоит в том, что на протяжении всего процесса проектирования должна существовать двунаправленная цепочка документации технических требований безопасности. Документация должна включать в себя не только проект, но и связанные с ним расчёты. Эта цепочка технических требований должна также распространяться на процессы производства, тестирования и обслуживания.

Документирование технических требований к безопасности при разработке аппаратной части

Механизация систем – ключевой документ для демонстрации интерфейсов связи с системой более высокого уровня. Цели обеспечения безопасности, а также ассоциированные с ними функциональные требования задаются на уровне автомобиля. Для разрабатываемого продукта функциональные требования безопасности наследуются либо из системы-автомобиля, либо из системы более высокого уровня. Функциональные требования должны быть чётко определены и преобразованы в технические требования к программным и аппаратным функциям.

К ключевым элементам документации механизации систем относятся:

- «флаг» функциональной безопасности титульного блока;
- номер для отслеживания документа;
- границы системы (электрические, механические, экзогенные);
- интерфейсы:
  - электрические (земля/питание, модификация мощности, коммуникационные шины, входные/выходные сигналы, напряжения/токи, скорости переключения, переходные величины / электромагнитная совместимость, импедансы);
  - механическое крепление (шок/вибрация);
  - поток воздуха;
  - поток охладителя;
- требования функциональной безопасности:
  - технические требования безопасности;
  - УПБА;
  - безопасное состояние (требуемые модели неисправностей/ответы);
  - интервал сбоеустойчивости;
  - предел обнаружения.

Каждый элемент, связанный с безопасностью, должен ссылаться на соответствующие технические требования к СБ и их ключевые атрибуты, влияющие на проект.

Заключение

Для проектирования транспортных средств, соответствующих современным требованиям безопасности, необходим интегрированный программный комплекс, основанный на единой базе данных, включающий в себя не только схемотехнический и топологический редакторы, а также средства моделирования, анализа и верификации, но и содержащий инструмент, обеспечивающий отслеживание требований и ограничений на всех этапах проектирования – от разработки технического задания и системного уровня до конечной реализации и моделирования.

НОВОСТИ МИРА

Прогноз развития электронной отрасли на 2017–2021 годы

По мнению аналитической компании IC INSIGHTS, рынок электронной техники автомобильного назначения останется в ближайшие годы «локомотивом» развития электронной отрасли, демонстрируя совокупный годовой прирост (CAGR), равный 6,4% в 2017–2021 гг. (при среднем по отрасли 4,6%), имея при этом всего 9,4% от мирового рынка электронных систем, оцениваемого в $1,62 трлн в 2018 году. Занимающая более половины рынка продукция телекома и компьютеры (31,8 и 25,8% соответственно) покажут более скромные цифры роста: +4,8 и +3,3%. Лидер прошлых лет – потребительская электроника – с ростом 4,5% попадает в отраслевой тренд, занимая при этом долю рынка в 12,1%. CAGR в 5,4% ожидается на рынке электронных систем промышленного и медицинского назначения – его доля составляет 14,5%. Заметно выросла доля электронных систем военного назначения: до 6,4%, но темпы роста здесь замедляются – CAGR не превысит 3,8%.

www.ecworld.ru

TESTING DAYS MOSCOW

Тематическая выставка – форум систем и технологий для автомобильных и авиационных испытаний и тестирования

Одновременно с
Control Days.Moscow

CONTROL DAYS MOSCOW

МОСКВА
Экспоцентр

2–4 апреля 2019

Акустика Ударные стенды
Пробоподготовка Аэродинамика
Мультиметры Телеметрия
Многоканальные измерительные системы
Анализаторы сигналов ЭМС
Испытания космических средств выведения
Испытательное моделирование
Испытания авиационных систем
Климатические испытания
Сенсорная измерительная аппаратура
Испытания автомобилей Виброиспытания
Моделирование ЛА Летные испытания
Механические испытания

При поддержке:
ЭКСПОЦЕНТР
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И КОНГРЕССЫ
МОСКВА

#testingdays_moscow

+7 (495) 78-601-78
www.testingdays.moscow