



Применение FMEA снижает риск в безопасных системах

Доктор Йозеф Бёрчек

Применение FMEA снижает риск в безопасных системах

Йозеф Бёрчек, HIMA GmbH + Co KG

Аннотация

Введение в действие стандарта МЭК 61508 привело к существенному росту требований к разработке и испытаниям безопасных систем. Вследствие этого возрастает роль моделей отказов при рассмотрении безопасности в таких системах. Результатом является создание моделей отказов с улучшенными характеристиками, позволяющими добиться значительных улучшений надежности всей системы уже на стадии проектирования и предлагающими сертифицирующему ведомству больше ясности и открытости в сочетании с легкостью понимания.

1 Введение

Возросшие запросы заказчиков и требований стандартов вместе с ужесточением законов в отношении охраны окружающей среды и ответственности изготовителя требуют от производителей и поставщиков больших усилий для изготовления надежных и безопасных систем. Для этого необходимы изделия с высокими характеристиками по безопасности и надежности, улучшенного качества, требующие меньших расходов и отвечающие последнему слову техники.

Изделия должны выполнять все обязательные требования законов и стандартов. Применявшиеся до настоящего времени системы обеспечения качества продукции и процессов опирались почти исключительно на опыт эксплуатации, т.е. на прошлое. Целью однако должно быть предупреждение возникновения отказов в будущем.

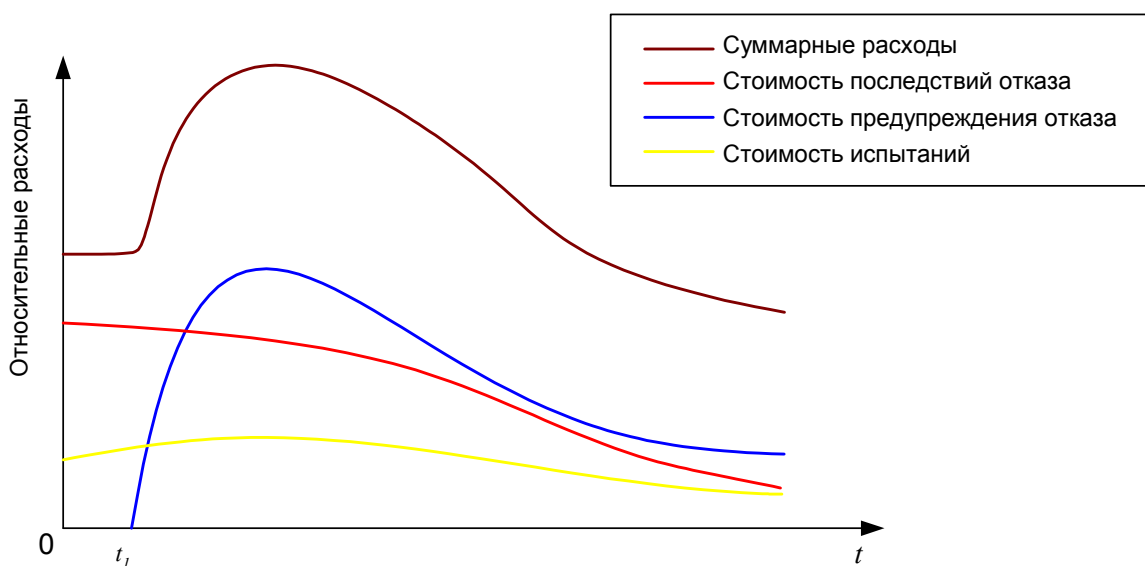


Рис. 1 Изменение соотношения между составляющими стоимости качества с течением времени. Момент t_1 обозначает начало использования методов обеспечения качества.

Обеспечение качества должно всегда быть упреждающе действующим методом. Поэтому оно должно играть существенную роль уже при проектировании изделия. При этом необходимо еще на стадии разработки и конструирования анализировать, какие отказы и с какими последствиями могут произойти, а также путем каких мер эти отказы могут быть предотвращены или последствия их возникновения ослаблены.

Предупредительные методы позволяют снизить издержки вследствие низкого качества, складывающиеся из стоимости испытаний, стоимости последствий отказов и стоимости мер по предупреждению отказов. На рис. 1 представлено изменение соотношения между указанными составляющими стоимости качества с течением времени. Расходы вследствие отказов и на испытания являются доминирующими до начала использования методов обеспечения качества (до момента t_1). С момента введения методов обеспечения качества (с момента t_1) общие расходы на качество сначала возрастают из-за появления расходов на меры по предупреждению отказов. При допущении, что число отказов в ходе создания изделия снижается (вызывая соответственно и снижение стоимости последствий отказов), в дальнейшем снижаются и суммарные расходы на качество.

К расходам на качество относится и стоимость устранения отказов. В этой связи здесь необходимо упомянуть о правиле десятикратного увеличения расходов на устранение отказов (rule of ten). Оно утверждает, что экономия расходов при рассмотрении суммарной стоимости системы тем выше, чем раньше в процессе проектирования будет обнаружен и устранен, или, еще лучше, предупрежден отказ.

2 Разработка и применение FMEA

Теория и практика анализа возможных причин и последствий отказов (FMEA, Failure Mode and Effect Analysis) была разработана в США в середине 60-х годов прошлого века управлением НАСА для программы «Аполлон». За прошедшее время методика успешно применялась в авиакосмической промышленности, атомной энергетике, автомобилестроении (концерн Форд был здесь первопроходцем), медицине, связи и даже при производстве бытовых изделий.

В 1980 году применение FMEA было стандартизовано в ФРГ. Сегодня эта методика находит широкое применение во всем мире в различных отраслях промышленности и стала неотъемлемой частью систем обеспечения качества. Примерами сфер особенно успешного применения FMEA для обеспечения качества являются разработки новых изделий или использование новых технологий, а также оценка критичных в отношении безопасности узлов и слабых мест. Другими областями применения являются внесение изменений в существующие изделия и исследования новых способов применения уже имеющихся продуктов.

2.1 Термины и определения

Для эффективного использования FMEA и получения оценки качества изделия или системы необходимо сначала принять некоторые определения. Особенно с понятиями надежность, безопасность и готовность часто возникает путаница или неправильная интерпретация.

2.1.1 Отклонение / отказ / дефект / заблуждение

Отклонение

Отклонением называется одно из состояний системы, которое является причиной отказа.

Отказ

Отказ является следствием отклонения от ожидаемого исполнения функции. При этом длительность эксплуатации не имеет значения, поскольку отказ может произойти уже при включении системы. Исходной предпосылкой для оценки отказа является полная работоспособность системы в момент начала анализа. Отказ может исследоваться по следующим критериям:

- **Вид отказа:** отказы делятся на внезапные отказы (например короткие замыкания, обрывы, ошибки функционирования), постепенные или дрейф параметров (рабочая точка системы вследствие влияния таких внешних воздействий, как температура или влажность, смещается настолько, что выходит за пределы разрешенного допуска) или перемежающиеся отказы (ограниченные во времени, исчезающие и снова появляющиеся отказы одного характера).
- **Причины отказов:** Причины отказов могут иметь различную природу, как то: ошибки эксплуатации, проектирования, изготовления, применения, обслуживания, другие, свойственные для данного изделия, а также амортизационные, первичные, вторичные и т.д.
- **Результаты отказов:** отказы могут проявляться в форме частичного, полного или критичного отказа, или оставаться без последствий.

При критичном отказе система больше не обеспечивает безопасности, поэтому воздействие отказа на защищаемую функцию может при этом оказаться самым непредсказуемым. В действующих стандартах по функциональной безопасности широко используются понятия *опасного* и *обнаруживаемого* отказа. Под опасным понимается такой отказ, который приводит систему в опасное состояние. Обнаруживаемый отказ может быть например зарегистрирован средствами встроенной диагностики.

Дефект

Причиной отклонения обычно является какой-либо дефект (например в аппаратуре или программном обеспечении), который постоянно или спорадически присутствует в системе.

Заблуждение

Заблуждением называют ошибку, вызванную неправильными действиями человека при совершении каких-либо действий в течении всего жизненного цикла системы. Такие ошибки обычно являются непредсказуемыми и приводят к отказу обслуживаемой системы.

Интенсивность отказов

Интенсивность отказов $\lambda(t)$ системы определяется как отношение вероятности отказа системы к периоду δt при наступлении отказа в период $[t, t+\delta t]$ при условии, что система была включена в момент $t = 0$ и в период $[0, t]$ работала безотказно:

$$\lambda(t) = -\frac{dR(t)/dt}{R(t)} = \frac{f(t)}{1-F(t)} \quad (1)$$

где

$$R(t) = 1 - F(t) \quad (2)$$

$$\frac{dR(t)}{dt} = f(t) \quad (3)$$

Здесь $R(t)$ обозначает функцию распределения вероятности безотказной работы, которая полностью определяется через интенсивность отказов $\lambda(t)$ следующим выражением:

$$R(t) = e^{-\int_0^t \lambda(\tau) d\tau}, \text{ откуда следует } R(t=0) = 1 \quad (4)$$

В самом общем смысле $F(t)$ обозначает функцию распределения во времени вероятности отказа и $f(t)$ соответственно плотность этого распределения для случайной величины (отказ какого-либо компонента системы), которые связаны между собой следующими выражениями:

$$F(t) = \int_0^t f(\tilde{t}) d\tilde{t} \quad (5)$$

при условии, что

$$\int_0^{\infty} f(\tilde{t}) d\tilde{t} = 1 \text{ и } \tilde{t} \geq 0 \quad (6)$$

Для стационарных процессов с постоянной интенсивностью отказов λ часто используемыми функциями распределения являются экспоненциальное распределение

$$F(t) = 1 - e^{-\lambda t} \quad (7)$$

и распределение Вейбулла – Гнеденко

$$F(t) = 1 - e^{-(\lambda t)^\beta} \quad (8)$$

где $\beta = 0.. \infty$ обозначает коэффициент, позволяющий точнее отразить реальное изменение функции распределения.

Риск

Риском R называется произведение плотности вероятности P наступления опасного события, которое приводит к возникновению ущерба, и степени нанесенного ущерба S (степень тяжести ущерба):

$$R = P \cdot S \quad (9)$$

Плотность вероятности P вычисляется при помощи правила произведения теории вероятностей, а именно из вероятности P_1 , описывающей вероятность наступления ущерба, и условной вероятности P_2 наступления ущерба, который однако не будет обнаружен:

$$R = P_1 \cdot P_2 \cdot S \quad (10)$$

В FMEA тоже анализируется степень риска наступления ущерба. Однако в FMEA определяется не вероятность наступления ущерба, а производится оценка степени опасности данного дефекта с помощью приоритетное числа риска RPZ (ПЧР). Уравнение (10) видоизменяется путем замещения составляющих его факторов P_1 , P_2 и S факторами A (частота наступления), E (частота обнаружения) и S (тяжесть последствий отказа). При этом коэффициенты A , E и S могут принимать целочисленные значения от 1 до 10:

$$RPZ = A \cdot E \cdot S \quad (11)$$

Безопасность

Понятие безопасности трактуется очень широко и зависит от области применения и использующей организации. Для всех определений однако является общим определение безопасности как состояния отсутствия опасности. Стандарт ФРГ VDE 0801 определяет безопасность как состояние, в котором отсутствует недопустимый риск нанесения ущерба. Таким образом состояние безопасности характеризуется тем, что имеющиеся риск не превышает определенного порогового уровня. При превышении этого уровня возникает критичное в отношении безопасности состояние.

2.1.2 Готовность

Готовность A (availability), точнее говоря, мгновенная готовность PA (point availability) определяется как вероятность выполнения системой в данных рабочих условиях и в данное момент времени требуемых от нее функций. Готовность является функцией надежности и ремонтпригодности, расчет которых как правило достаточно сложен. Исходя из стационарного рабочего состояния – система находится либо в нормальном функционировании при нормальных условиях или в ремонте – коэффициент мгновенной готовности сходится к постоянной величине, которая независимо от начального состояния в момент $t = 0$ равна

$$V = \lim_{t \rightarrow \infty} PA = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF} \quad (12)$$

Здесь описывает параметр $MTTF$ (mean time to failure) среднюю наработку на отказ, $MTTR$ (mean time to repair) среднюю длительность проведения ремонта. Введя параметр $MTBF$ (mean time between failures) как средний интервал времени между наступлением отказов с учетом времени на ремонт, получим

$$MTBF = MTTF + MTTR \quad (13)$$

Наряду с коэффициентом мгновенной готовности, который здесь для простоты именуется готовностью, существуют другие виды готовности, как например средняя готовность, объединенная готовность или готовность исполнения предназначения. Эти виды определяются в зависимости от области применения описываемой ими системы. На практике повышение готовности системы обычно происходит путем резервирования. Архитектура системы с резервированием выполняется таким образом, что отказ одного компонента не влияет на функциональность системы. Необходимо учитывать однако, что повышение готовности не приводит автоматически к повышению надежности. Надежность систем с избыточностью и готовностью определяется тестами и диагностикой, проводимыми в безостановочном режиме.

2.1.3 Надежность

В настоящей работе надежность рассматривается как вероятность, характеризующая степень поддержания непрерывного функционирования системы в течении определенного времени T . Понятие надежности понимается – в соответствии со стандартами MIL-STD 721 и МЭК 271 – как синоним вероятности выживания. Надежность однако ничего не говорит о безопасности системы. Также и ненадежные системы могут быть безопасными, если отдельные отказы действуют на систему в безопасном направлении: например, обесточивают выходы модуля (отсутствие энергии на выходах считается безопасным состоянием).

Надежность характеризуется в математике функцией надежности $R(t)$ (не путать с величиной риска R). Функция надежности $R(t)$ полностью определяется интенсивностью отказов $\lambda(t)$. Справедливо следующее

$$R(t) = e^{-\int_0^t \lambda(\tau) d\tau}, \text{ где } R(0) = 1 \quad (14)$$

Одним из важнейших параметров надежности является математическое ожидание длительности отрезка времени до первого отказа системы, более известное как среднее время наработки до отказа и обозначаемое как $MTTF$ (mean time to failure). Взаимосвязь между $MTTF$ и $R(t)$ описывается уравнением

$$MTTF = \int_0^{\infty} R(t) dt \quad (15)$$

Вывод данного уравнения приведен в литературе. В случае экспоненциального закона распределения (означающего постоянство интенсивности отказов $\lambda(t) = \lambda$) справедливо

$$MTTF = \frac{1}{\lambda} \quad (16)$$

Данное уравнение однако является не определением, а расчетным выражением и справедливо только для экспоненциального закона распределения!

3 FMEA

В обеспечении качества применяются различные методы для распознавания отказов, как например:

- анализ деревьев отказов (FTA, fault tree analysis)
- анализ деревьев событий (ETA, event tree analysis)
- анализ видов и последствий отказов АВОП (FMEA, failure mode and effects analysis)

Дальнейшее изложение концентрируется только на принципе FMEA. С помощью FMEA исследуются виды и причины отказов деталей, компонентов и процессов вместе с их воздействием на систему. В отличие от анализа деревьев отказов здесь исследуются отказы отдельных компонентов вместо комбинаций отказов. В то время как анализ деревьев отказов проводится по принципу сверху вниз, в FMEA используется принцип снизу вверх. Это означает, что анализ проводится, исходя из дефектов отдельных компонент и ошибок рабочих операций, с рассмотрением в последующем их влияния на систему в целом. При этом при помощи системного формализованного подхода должны быть по возможности охвачены все потенциально возможные дефекты. Наряду с документированием потенциальных дефектов дополнительной целью анализа является качественная оценка систем, продукции или процессов в отношении обнаружения дефектов отдельных элементов или технологических этапов. Рассмотрение и оценка типов и причин потенциальных дефектов позволяет надеяться на ранее обнаружение слабых мест. При оценке дефектов учитываются также вызванные этими дефектами отказы.

Путем анализа должны быть предотвращены дефекты, устранение которых будет тем дороже, чем позднее в течении эксплуатации оборудования они будут обнаружены. Кроме того – данный аспект особенно важен для безопасных систем – предупреждение возникновения дефектов предназначено для повышения безопасности и надежности используемой системы. В документацию FMEA могут включаться предложения по предотвращению отказов для смягчения их последствий или снижения вероятности их наступления. Дальнейшие доводы в пользу FMEA как метода обеспечения качества:

- Разработчики приобретают лучшее понимание структуры исследуемой системы и влияния факторов, существенно определяющих надежность системы.
- На базе FMEA проще принимать решения о внесении небольших изменений для улучшения системы.
- В отношении изготовления, эксплуатации и техобслуживания могут быть рекомендованы или выбраны меры, обеспечивающие правильное применение изделия.
- Заказчик получает уверенность, что приобретенное им изделие соответствует его представлениям в отношении надежности.

3.1 Основные виды FMEA

Применение FMEA должно гарантировать вовлечение в рассмотрение любого возможного дефекта с принятием мер против возникающих дефектов при строгом ведении документации. Он основывается на теоретических, научных и практических

знаниях и дополняется в стадии проведения испытаний опытом происходящих отказов. Некоторые принятые к рассмотрению теоретически возможные дефекты бывает необходимо создавать путем специальных испытаний.

Принято различать три области применения FMEA, которые частично перекрывают друг друга и определяются областью использования:

- FMEA системы
- FMEA конструкции
- FMEA процесса

При FMEA системы, называемой также FMEA продукта, анализируется система в целом. На основании технического задания исследуются принципы построения узлов и компонентов системы без подробного рассмотрения примененных деталей и элементов. Целью является моделирование функционального взаимодействия узлов и компонентов системы и стыков их взаимодействия для предупреждения ошибок при выборе и расчете системы и учета источников опасности периферийного оборудования. При FMEA конструкции, называемой также FMEA проектирования, проводится анализ узлов на уровне составляющих их компонентов и деталей. Входящие в узел детали исследуются на предмет правильности их конструктивного расчета и оптимальности выполнения заданных функций. Для этого сначала описывается узел и выполняемая им функция, включая стыки взаимодействия с другими частями конструкции при принятии допущения, что функции внешних стыков работают безупречно. После этого анализируются возможности дефекта какой – либо детали и последствия этого дефекта как на функцию самой детали так и на сохранение безопасности в компонентах данного узла и вышестоящих уровней конструкции. Одновременно здесь также показываются возможные пути решения возникающих проблем.

FMEA конструкции выполняется инженерами–разработчиками изделия на этапе разработки и чем раньше тем лучше. Определенным преимуществом является, если FMEA выполняется другим специалистом, чем тот, кто участвует в разработке. Таким образом обеспечивается новизна взгляда на конструкцию и принятие во внимание любой возможной ошибки или дефекта. Области применения FMEA конструкции являются:

- Выработка качественной или количественной характеристики достижимой вероятности возникновения дефекта
- Сравнение вероятности возникновения дефекта в альтернативных концепциях решений
- Нахождение слабых мест в проекте, т.е. таких узлов или деталей проекта, которые являются критичными в отношении их влияния на общую надежность
- Текущие повторные проверки способности обеспечения качества выбранной конструкции, имеющие целью сохранение возможности своевременно предпринять необходимые меры по улучшению конструкции.

При FMEA процесса проводится анализ планирования и реализации процесса изготовления изделия. Благодаря этому можно обеспечить отсутствие ошибок планирования и процесса производства. Для этого сначала подробно и без пропусков описывается каждый шаг процесса, причем сам процесс делится на отдельные законченные технологические операции. Предпосылкой здесь является, как и при FMEA конструкции, отсутствие дефектов продукции после предыдущей технологической операции. Проведение FMEA процесса начинают одновременно с планированием самого процесса для исследования необходимого для производства продукции оборудования на пригодность его применения. Результаты FMEA должны быть готовы до принятия решения о закупке выбранного технологического оборудования. Таким образом, FMEA процесса служит в первую очередь для предупреждения ошибок производства и обеспечения соответствующего качества продукции.

Взаимосвязь между различными видами FMEA представлена на рис.2. Высший уровень абстрагирования занимает FMEA системы, в то время как FMEA процесса находится на низшем уровне. Между ними находится FMEA конструкции. Каждый вид FMEA

проводится для своего уровня. На рис. 2 показано также перемещение причинно-следственной связи с одного уровня на другой. То, что является следствием на лежащем ниже уровне FMEA, служит причиной для уровня, находящегося выше. Из рис. 2 видно, что иногда бывает полезно дальнейшее разделение уровней рассмотрения для одного и того же типа FMEA. В следующем примере FMEA системы разделен на два уровня.

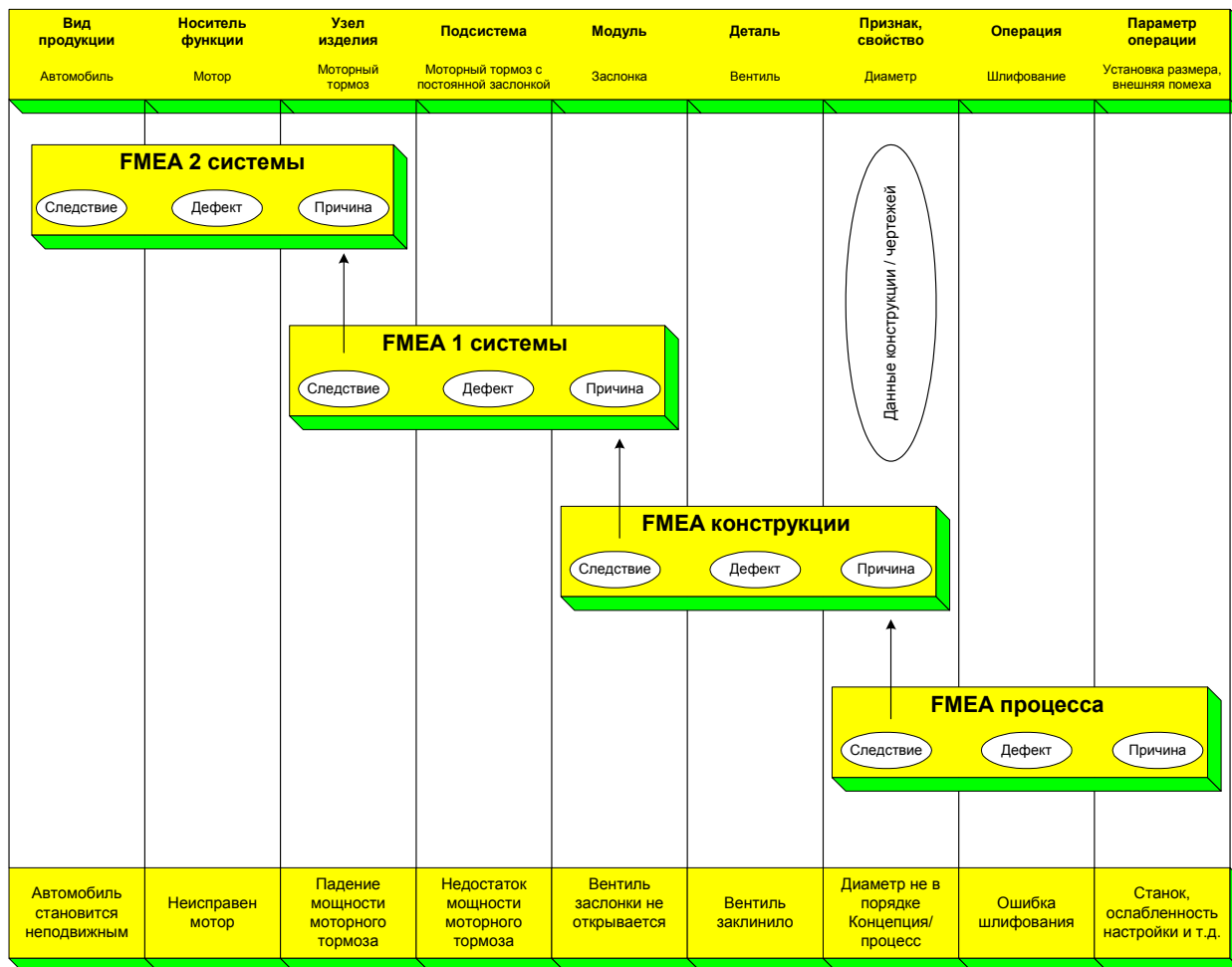


Рис. 2 Взаимосвязи между различными видами FMEA

Причинно-следственная цепочка демонстрируется на примере взаимосвязи между FMEA процесса и конструкции: в то время как в FMEA конструкции допускается неисправность процесса изготовления (диаметр вентилья слишком мал) как причина определенного дефекта (вентиль дросселя не открывается), этот же дефект в FMEA процесса рассматривается как следствие. В FMEA процесса определяется, какая причина лежит в основе этого дефекта. В описываемом примере причиной является неправильная настройка станка. В дальнейшем изложении акцент будет делаться на рассмотрении FMEA конструкции, поскольку именно она чаще всего применяется в департаментах проектирования производителей.

4 Различия между общей и специализированной FMEA и возможности улучшения изделия

Принципиально различают между общим и специальным FMEA, например специальным FMEA конструкции. Общий FMEA (Рис. 3) можно разделить на три части:

- Описание системы
- Анализ дефектов
- Действия

В специализированном FMEA (рис.4) дополнительно рассматриваются еще два пункта:

- Оценка риска
- Оценка результата

В то время как оценка риска происходит после анализа ошибок, оценка результатов может происходить только после окончания проведения контрольных испытаний.

В дальнейшем будет подробнее рассмотрен FMEA конструкции в том виде, в котором он может применяться при проектировании безотказных электронных устройств. Под безотказными электронными устройствами здесь понимаются такие устройства, возникновение отказа в которых распознается аппаратным или программным путем и имеет следствием перевод устройства в определенное безопасное состояние. Таким образом в отношении безопасных электронных устройств вопрос стоит не о предотвращении отказа, а только о его распознавании. Дефект, возникающий в аппаратуре, должен распознаваться в любом случае. По этой причине можно исключить из специального FMEA положение о предупреждении дефекта, которое по идее должно присутствовать в любом общем FMEA, независимо от того, является ли он FMEA системы, конструкции или процесса (Рис. 3, столбец 8). Вместо пункта «Предупреждение отказа» в столбец 8 специальной FMEA (Рис. 4) вводится пункт «Интенсивность отказов».

Фирма		FMEA Конструкции <input checked="" type="checkbox"/> Процесса <input type="checkbox"/> Системы <input type="checkbox"/>			Модель / система				Номер внесенного изменения				
Дата		Проверено		Дата		Выполнено		Дата		Кем внесено	Дата		
Состояние в настоящее время													
1	2	3	4	5	6	7	8	9			14		
№ системы, детали	Элемент	Функция	Возможный дефект, вид дефекта	Возможные причины дефекта	Возможные последствия дефекта	Распознавание дефекта	Интенсивность отказов	Оценка дефекта			Оценка после проведенного испытания		
Описание системы			Анализ дефектов										
										10	11	12	13
										Область ответственности	Распознавание дефекта	Интенсивность отказов	Контрольное испытание
										Проводимые мероприятия			

Рис. 3 Пример выполнения общего FMEA с оценкой дефекта, но без оценки риска

Следующее отличие состоит, как уже упоминалось, в оценке степени риска. Ранее приоритетное число риска ПЧР не рассчитывалось – что и не было необходимым! Из-за этого однако терялся шанс документировать дальнейшее улучшение устройства / конструкции в отношении повышения качества. Колонка 11 «Приоритетное число риска ПЧР» замещает колонку 9 «Оценка» из общего FMEA. Если имеется только общий FMEA, то обнаружение отказа рассматривается следующим образом: Если дефект будет обнаружен аппаратным или программным путем и устройство будет переведено в безопасное состояние, то колонка «Оценка» не заполняется. Для случая, если критичный в отношении безопасности дефект не будет обнаружен аппаратным или программным путем и устройство соответственно не будет переведено в

Тяжесть последствий наступления дефекта S оценивается на основе десятибалльной шкалы. Оценка отражает влияние последствий дефекта на систему. Виды дефектов с одинаковыми последствиями должны также одинаково оцениваться. При определении оценки исходят из того, что дефекта возник, но не был обнаружен. Для присвоения правильного балла рекомендуется использовать оценочные таблицы Объединения немецкой автомобилестроительной промышленности (VDA, Verband der deutschen Automobilindustrie). Баллы от 1 до 8 характеризуют возрастающий размер ущерба, баллы 9 и 10 означают недопустимое состояние системы (например, нарушения законодательные предписания) или характеризуют критичное в отношении безопасности последствие возникновения дефекта. Одновременно рассматривается вероятность возникновения A причины дефекта, которая также оценивается тоже по десятибалльной шкале. При оценке исходят из того, что причина дефекта и сам дефект остаются необнаруженными вплоть до отгрузки изделия заказчику. При оценке вероятности возникновения дефекта учитываются предупредительные меры для исключения дефектов (меры по борьбе с возникновением причин дефектов или препятствующие их возникновению), которые считаются эффективными. Для оценки A рекомендуется использование соответствующих таблиц VDA для FMEA конструкции или процесса. Оценка ориентируется по шкале возможной интенсивности отказов. Интенсивность отказов λ опирается на число дефектов, ожидаемое в течении запланированного жизненного цикла рассматриваемого компонента. Вероятность обнаружения E дефекта также определяется и оценивается на основании десятибалльной шкалы. Здесь необходимо оценить эффективность контрольно-испытательных мероприятий по обнаружению дефекта. Для определения приоритетного числа риска ПЧР (RPZ) вычисляется произведение

$$RPZ = S \cdot A \cdot E \quad (17)$$

Максимальное теоретическое значение приоритетного числа риска равно 1000. На практике обычно ориентируются на предельное значение равное 125. Это значение однако не является универсальным, поскольку в различных областях как сам верхний предел, так и соответствие критериев оценки на шкале для S , A и E носят различный характер. Необходимо далее учитывать, что индивидуальные оценки для S , A и E не должны превышать 8 баллов без того, чтобы провести повторную обстоятельную проверку:

- $S > 8$ Недопустимое состояние системы / нарушение законодательных предписаний, риск для безопасности
- $A > 8$ Дефект с особенно частым возникновением
- $E > 8$ Трудно или совершенно не обнаруживаемый дефект

5.2 Проводимые мероприятия

Другой целью FMEA является использование его в виде каталога требований для тестового программного обеспечения по обнаружению дефектов аппаратуры, а также как документальное подтверждение результатов проведенных контрольных испытаний аппаратуры (см. колонки «Требования к тестовому программному обеспечению», «Проверка тестового программного обеспечения» или «Контрольные испытания» на рис. 3 и 4). Для ответственного инженера, который интенсивно исследует с помощью FMEA свою разработку, значительно проще составить техническое задание на тестовое программное обеспечение уже на данном этапе, чем это делать уже после завершения своей разработки. Дополнительным преимуществом является и более раннее начало создания программного обеспечения, приводящее к одновременной совместной работе разработчиков аппаратуры и программистов. После того как конструктор оформил соответствующее техническое задание, следующим логическим шагом для него является выработка спецификации для проверки создаваемого программного обеспечения. После контрольных испытаний аппаратуры и подтверждения предполагаемых дефектов как действительно не критичных, эти дефекты могут быть внесены в FMEA с пометкой «не критично». При необходимости заново

определяются вероятность возникновения A и/или степень тяжести последствий S . Контрольные испытания необходимы особенно тогда, когда дефекты не возникают в самом устройстве, а искусственно создаются тестовым программным обеспечением, которое же и должно их обнаруживать.

5.3 Оценка результатов / улучшение качества

После проведения контрольных испытаний может сложиться ситуация, что принятые при оценке риска прикидки должны будут откорректированы, потому что вероятность возникновения оказалась меньше или больше принятой или была неправильно заложена тяжесть последствий.

Для приоритетных чисел риска $RPZ > 125$ и / или отдельных оценок для S , A или $E > 8$ необходимо выработать меры по улучшению изделия. Здесь возникают различные принципиальные подходы, которые разнятся в их эффективности и степени воздействия на оценки величин S , A или E :

- Недопущение возникновения причин отказа $\Rightarrow A = 1$
- Создание препятствий на пути возникновения причин отказа $\Rightarrow A$ уменьшается
- Уменьшение влияния последствий отказов $\Rightarrow S$ уменьшается
- Повышение вероятности обнаружения отказов $\Rightarrow E$ уменьшается

Мерам по предупреждению отказов необходимо по экономическим соображениям отдавать предпочтение перед мерами по обнаружению отказов. Хотя меры по обнаружению отказов и повышают вероятность обнаружения, они не ведут непосредственно к улучшению качества. Также далеко от идеала снижение тяжести последствий отказов, поскольку оно требует больших затрат. Как правило, тяжесть последствий в основном снижают конструктивными мероприятиями, например резервированием. Поэтому снижение количества возможных дефектов должно быть первоочередной задачей мер по улучшению качества. При этом важно четко прояснить распределение ответственности и контроля участвующих сторон. Разработанные меры по улучшению качества должны быть зафиксированы в плане реализации с привязкой по времени и исполнителям с учетом длительности их реализации и ожидаемой стоимости.

В оценке результатов должны быть документированы результаты мер по улучшению качества. Для этого повторно проводится оценка степени риска. Улучшение качества считается достигнутым, если новое приоритетное число риска после переработки изделия имеет меньшее значение чем раньше. После реализации запланированных мер параметры оценок нового улучшенного состояния переносятся в актуальное описание и вносятся в формуляр FMEA.

6 Выводы и заключение

На сегодняшний день FMEA применяется во всем мире в различных отраслях промышленности и стал неотъемлемой частью систем обеспечения качества. Особенно необходимо проводить FMEA при создании новых производственных процессов для проверки обеспечения ими требуемого качества продукции. К задачам по обеспечению качества относятся среди прочего обнаружение и предупреждение функционально слабых и критичных в отношении безопасности мест и создание документации по обеспечению качества.

Различают три области применения FMEA, переходящие друг в друга и зависящие от конкретного применения:

- FMEA систем (изделия)
- FMEA конструкции (разработки)
- FMEA процесса

Кроме того еще различают еще

- общий FMEA
- специальный FMEA

Наряду с вышеперечисленным FMEA служит также в качестве подтверждения проведенных контрольных испытаний и в виде перечня требований для тестового программного обеспечения.

Для оформления сертификации безопасных модулей в сертифицирующем ведомстве заявитель должен предъявить наряду с FMEA также протоколы контрольных испытаний аппаратуры. Какой объем испытаний необходим для сертификации нового продукта? основополагающими документами для планирования и проведения контрольных испытаний по функциональной безопасности модулей для всех участвующих в сертификации сторон являются в ФРГ следующие документы:

- DIN V 19250
- DIN V VDE 0801
- IEC/EN 61508 (МЭК 61508 Функциональная безопасность)

Кроме того для успешной сертификации сертифицирующее ведомство использует обычно также следующие документы:

- Спецификацию изделия и структуры обеспечения его безопасности
- Описание работы аппаратуры, принципиальные схемы, перечни элементов, чертежи трассировки и монтажные схемы
- Результаты FMEA изделия и его компонентов, спецификация контрольных испытаний аппаратуры, при необходимости вместе с протоколами проведенных испытаний
- Описание архитектуры программного обеспечения, порядок и протоколы тестовых испытаний программного обеспечения
- Действующие на фирме процедуры проектирования, протоколы отслеживания версий и внесения изменений в аппаратуру и программное обеспечение.
- Руководства пользователя (включая руководства по программированию), изготовленные модули с описанием испытательного оборудования

Из перечисленного видно, что FMEA играет существенную роль в создании и предложении на рынке сертифицированных изделий с высоким уровнем качества.

Литература

- [1] МЭК 61508 Функциональная безопасность
- [2] *Biolini, A.*: Zuverlässigkeit von Geräten und Systemen, Springer Verlag, 1997
- [3] *Börcsök, J.*: Elektronische Sicherheitssysteme – Hardwarekonzepte, Modelle und Berechnungen. Hüthig Verlag, 2004
- [4] *Börcsök, J.*: Internationale-/Europe Norm 61508, Vortrag bei der VD-Tagung der HIMA GmbH + Co KG, 2002
- [5] *Börcsök, J.*: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen; Universität Kassel, 2002
- [6] *Börcsök, J.*: Sicherheits-Rechnerarchitekturen Teil 1 und 2, Vorlesung Universität Kassel; 2000/2001
- [7] *Börcsök, J.*: Echtzeit-Betriebssysteme für sicherheitsgerichtete Realzeitrechner, Vorlesung Universität Kassel, 2001
- [8] DIN VDE 0801: Funktionale Sicherheit sicherheitsbezogener elektrische/elektronische/programmierbarer elektronischer Systeme (E/E/PES), (IEC 65A/255/CDV:1998)
- [9] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutheinrichtungen. Beuth Verlag, Berlin, 1998
- [10] DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben. Beuth Verlag, Berlin, 1984
- [11] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung. Beuth Verlag, Berlin, 2000

Об авторе



Приват-доцент д-р Йозеф Бёрчек (44) руководит департаментом проектирования фирмы HIMA GmbH + Co KG, производящей системы автоматизации промышленности. Более 9 лет он специализируется в области безопасной вычислительной техники и участвует в работе различных комитетов Немецкой комиссии по стандартизации в электротехнике, электронике и информационной технике (составной части DIN и VDE). С 1992 он читает лекции в университетах и институтах на темы автоматизации, микропроцессоров, систем реального времени, ЭВМ и архитектур безопасных ЭВМ.

Адрес: HIMA Paul Hildebrandt GmbH + Co KG, Albert-Bassermann-Str. 28, D-68782 Brühl bei Mannheim, тел. +49-6202-709-270, адрес электронной почты: j.boercsoek@hima.com