Взаимосвязь между стандартами CENELEC в области железнодорожной сигнализации и другими стандартами по безопасности

Йенс Брабанд,

Юдзи Хирао,

Джонатан Ф. Людеке

Несмотря на существование большого количества различных международных, европейских, японских и американских стандартов по безопасности, эти стандарты во многих общих аспектах и концепциях совпадают. Имеется, однако, ряд различий в деталях, например, в то время как концепции TFM, THR и MTTHE в значительной степени аналогичны в части задания целевых показателей безопасности, процедура верификации, обеспечивающая доказательство соответствия этим целевым показателям, оказывается различной.

Наиболее важные различия заключаются в следующем:

- Концепция SIL (Safety Integrity Level = «уровень целостности безопасности» или «уровень соответствия комплексу требований безопасности») не является общепринятой на железнодорожном транспорте США.
- В Японии для оценки безопасности вместо количественных методов анализа и абсолютных целевых показателей в большей степени применяются качественные методы анализа, включающие анализ угроз (hazard), а количественные методы анализа применяются в целях подтверждения.
- Отношение к стандартам и их применение. Иногда стандарты рассматриваются как руководящие указания, а иногда - как обязательные правила.
- Терминология.

Авторы надеются, что будущие обсуждения приведут к большей гармонизации на международном уровне.

Введение

Со времени проведения сбора отзывов по ранним проектам стандартов в середине 1990-х годов стандарты CENELEC по железнодорожной сигнализации, в особенности, подмножество стандартов, относящихся к функциональной безопасности [1, 2, 3, 4], привлекли к себе всеобщее внимание. Причины этого разнообразны, но наиболее важные из них следующие:

- Во-первых, они представляют единственные истинно международные стандарты в данной области, разработанные членами CENELEC, которых теперь 22 и каждый из которых представляет одну из европейских стран, с участием сотен экспертов.
- Во-вторых, в то время как применение стандартов, например, стандартов МЭК (IEC), во многом осуществляется по усмотрению

операторов и поставщиков, стандарты CENELEC сделаны «де факто» обязательными директивой Европейского Союза (ЕС) № 93/38/ЕЕС, которая требует, чтобы все контракты на сумму более 400,000 € заключались по итогам тендеров, проводимых на основе европейских спецификаций (включая европейские стандарты).

Интерес к стандартам CENELEC за последние несколько лет резко возрос по следующим причинам:

- Весьма вероятно, что в ближайшем будущем эти стандарты станут всемирными стандартами МЭК (IEC) с помощью процедуры «быстрого принятия» (fast-track), что сделает их первыми всемирными стандартами в данной области.
- Новая директива ЕС от 3 декабря 2001 г. № 2001/95/ЕС «Общая безопасность изделий» (General Product Safety) предъявляет требование усиления роли стандартов по безопасности изделий по сравнению с предшествующим документом, директивой «Ответственность за изделия» (Product Liability) от 25 июля 1985 г. № 85/374/ЕЕС. В соответствии с новой директивой «изделие следует считать безопасным ..., если оно соответствует ... европейским стандартам, ссылки на которые опубликованы Комиссией в Официальном журнале Европейского Сообщества ...».

Это означает, что в долгосрочной перспективе стандарты CENELEC, весьма вероятно, станут единственными стандартами, имеющими значение для железнодорожной сигнализации, на международном рынке, поскольку глобальные поставщики, с одной стороны, не будут иметь возможности продолжать учитывать большое число разных местных стандартов, а, с другой стороны, заказчики желают обеспечивать на проводимых ими тендерах максимально возможную степень конкуренции. Стандарты CENELEC служат интересам обеих сторон в максимальной степени.

Основное внимание в настоящей статье уделяется взаимосвязи между стандартами CENELEC и другими стандартами по безопасности, как национальными, так и общими международными стандартами. Эта взаимосвязь важна потому, что в перспективных применениях стандартов CENELEC не будет возможности считать, что оборудование уже сертифицировано на основе стандартов CENELEC. Вместо этого будет необходимо разрабатывать системы, которые могут быть сертифицированы в соответствии со стандартами CENELEC, из компонентов, ранее сертифицированных на основе национальных или других международных стандартов. Это означает, что знание взаимосвязей и зависимостей между стандартами окажется преимуществом при решении такой задачи.

Об аналогичной работе уже сообщалось ранее одним из авторов [5], но лишь применительно к предварительным редакциям некоторых стандартов. Исследование, завершенное в 1995 г., имело целью идентификацию (выявление) наилучшей методики верификации (verification) и проверки соответствия требованиям (validation) (процедуры «V&V») и привело к заключению, что документы, содержащие прежде всего наиболее существенные показатели с точки зрения процедур верификации (verification)

и проверки соответствия требованиям (validation), т. е. процедуры «V&V», по безопасности, в тот период времени включали:

- IEC 65A 122 [6] и 123 [7] (редакции проекта стандарта IEC 61508 [8]);
- проекты стандартов CENELEC prEN 50128 и prEN 50129;
- руководящие указания Германских железных дорог Mü8004 [9];
- военные стандарты Великобритании Def Stan 00-55 [10] и Def Stan 00-56 [11];
- военный стандарт США MIL-STD-882C [12].

1. Генеалогия стандартов CENELEC

Как и в случае контактов между людьми, когда может быть полезным знать побольше о семье данного человека, чтобы лучше понять его поведение, так и применительно к стандартам такое знание также может представлять интерес, поскольку стандарты создаются не изолированно, а используют идеи друг друга. На *рис. 1* приведены основные «корни» стандартов CENELEC в той мере, в какой они известны авторам.

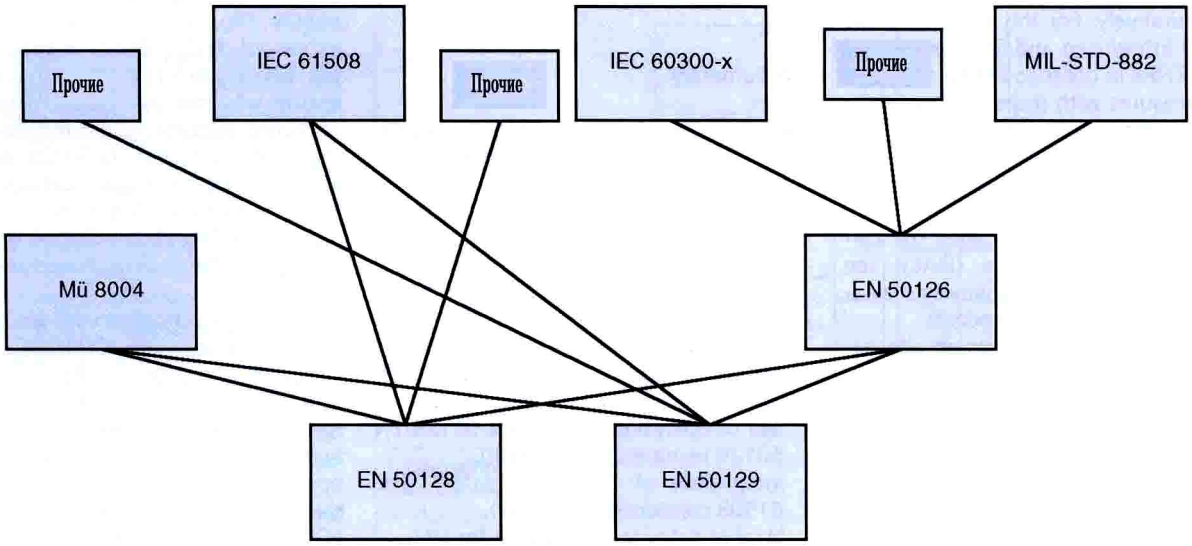

Рис. 1. «Дерево семейства» основных стандартов CENELEC

Очевидно, что самое существенное влияние оказала публикация МЭК по безопасности IEC 61508, установившая основные определения и подходы к функциональной безопасности для всех областей применения. Это влияние будет рассмотрено в следующих разделах.

Крупный вклад, особенно в режим доказательства соответствия требованиям безопасности (Safety Case), предписываемый стандартом EN 50129 [3], сделали руководящие указания Германских железных дорог Mü8004. Структура отчета о технической безопасности (Technical Safety Report), а еще в большей степени его содержание, непосредственно перенесены в стандарт EN 50129 из руководящих указаний Mü8004. Это является основным отличительным фактором по сравнению со стандартом IEC 61508, поскольку стандарт IEC 61508 не содержит четкой структуры доказательства соответствия требованиям безопасности (Safety Case), которая

является вэжным условием для «перекрестной приемки» [cross-acceptance: статус изделия после прохождения им приемки одной Администрацией в соответствии с действующими европейскими стандартами, характеризующийся допустимостью («приемлемостью») данного изделия и для других Администраций без необходимости дальнейшей оценки (экспертизы).].

Другой важной характеристикой стандартов CENELEC является наличие в них набора показателей управления RAMS (надежности, оперативной готовности, пригодности к техническому обслуживанию и безопасности = Reliability, Availability, Maintainability and Safety). В этой части основной вклад в стандарт EN 50126 [1] сделали военный стандарт США MIL-STD-882 (иногда его называют «матерью» всех стандартов управления безопасностью) и серия стандартов IEC 60300 [13], относящихся к управлению и методам обеспечения «обобщенной надежности» (dependability: дословно «возможность положиться на...»). Следует отметить, что, согласно терминологии МЭК (IEC) термин «dependability» является общим («коллективным») термином для надежности (reliability), доступности (оперативной готовности = availability) и пригодности к техническому обслуживанию (ремонтопригодности = maintainability), в терминологии CENELEC обозначаемых совместно сокращением «RAM» (Reliability, Availability, Maintainability). В действительности то, что вопросы безопасности (safety) и «обобщенной надежности» (dependability) в системе стандартов МЭК (IEC) оказываются отнесенными к двум разным стандартам, разработанным разными техническими комитетами, является недостатком этой системы стандартов.

2. Сравнение основных концепций стандарта IEC 61508 и стандартов CENELEC

Стандарты CENELEC представляют собой адаптацию стандарта IEC 61508 для железнодорожного транспорта. Представляет интерес, однако, знание, в каких отношениях они совпадают и в каких отличаются.

2.1 Определение безопасности и анализ рисков

В стандартах IEC 61508 и EN 50126/EN 50129 для анализа угроз (hazard) и рисков (risk) используется одно и то же определение безопасности, основанное на риске. В обоих стандартах приведены примеры методов, но не предписывается использовать какой-либо конкретный метод или критерий допустимости риска. Их целью является устранение угроз и, если это практически невыполнимо, снижение риска.

Конкретное преимущество стандартов CENELEC заключается в том, что, в соответствии со стандартом EN 50126, мероприятия в части показателя RAM (Reliability, Availability, Maintainability) и в части безопасности рассматриваются совместно, в том числе и с точки зрения управления показателями RAMS [14].

2.2 Системное определение и целевые показатели безопасности

Стандарт IEC 61508 устанавливает целевые показатели (targets) для функций электрических/ электронных/программируемых электронных систем управления (Э/Э/ПЭС = E/E/PES, electrical/electronic/programmable electronic

control system). В нем четко определено, какие компоненты являются частью таких систем: датчики, логические решающие устройства, каналы связи и исполнительные устройства. Это определение взято из области автоматизации производственных процессов. Однако, для других областей применения оно может применяться лишь ограниченно, так как системы оказываются значительно более сложными, нежели в области автоматизации производственных процессов.

В общем, стандарты EN 50126 и EN 50129 устанавливают целевые показатели для угроз (hazards), которые могут возникнуть на любом уровне системы. В стандарте EN 50129 окончательно определены требования к целостности безопасности (safety integrity) на функциональном уровне, аналогичном уровню, для которого заданы целевые показатели в стандарте МЭК (IEC).

2.3 Меры целевых показателей

В стандарте IEC 61508 определена мера целевого показателя отказов (Target Failure Measure = TFM), включающая как случайные, так и систематические отказы. Мера TFM определена в количественном отношении и является эквивалентной уровню целостности безопасности (Safety Integrity Level = SIL). Принимается, однако, что количественно может быть определена лишь целостность в отношении случайных отказов, в то время как целостность в отношении систематических отказов должна учитываться качественно. В стандарте IEC 61508 делается различие между работой системы в режиме «малой нагрузки» («низкого спроса» = low demand) и в непрерывном (continuous) режиме, для которых определены различные значения TFM.

Допустимые уровни угроз (Tolerable Hazard Rates = THR) в стандарте EN 50129 являются обобщением TFM из стандарта IEC 61508, поскольку они иогут быть определены для любого уровня архитектуры системы. Для функций непрерывного (continuous) режима работы понятия TFM и THR идентичны, и таблицы уровней целостности безопасности (SIL) одни и те же. Графическое обобщение приведено на *рис. 2*.

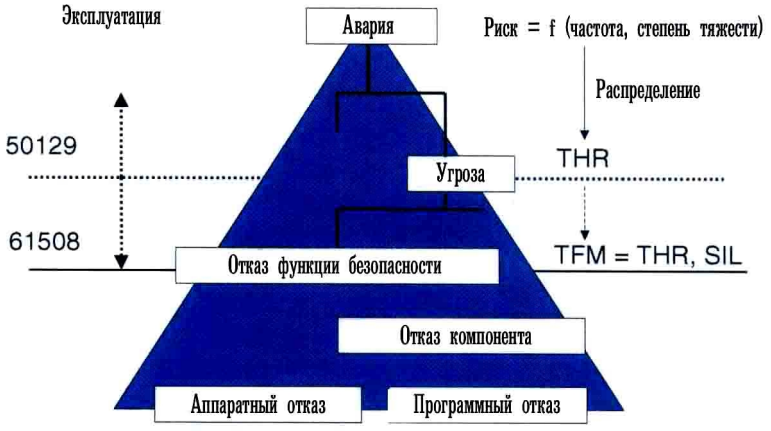

Рис. 2. Аналогия между стандартами IEC 61508 и EN50129 в части мер целевых показателей

Важно отметить, что, по определению, показатели THR включают как случайные, так и систематические отказы и являются целевыми показателями для обоих видов отказов. При этом, однако, учитывается, что, в соответствии с текущим современным состоянием данной области количественной проверке (верификации) поддается только вклад случайных отказов. По этой причине введена концепция уровней целостности безопасности (SIL), при этом показатели SIL выводятся из показателей THR с целью определения требований достаточности к контрмероприятиям в части систематических отказов. Это можно считать недостатком, но изучение стандартов на программное обеспечение показало, что в настоящее время альтернативы такому подходу нет [15]. Интересно отметить, что в гражданской авиации также используется аналогичное понятие, называемое «Development Assurance Level» (DAL = «Уровень (безопасности), гарантируемый при разработке»). Сравнение принципов и стандартов безопасности, применяемых на железнодорожном транспорте и в авиации, приведено в работе [16].

Другой вывод заключается в том, что в качестве альтернативы понятию THR можно было бы использовать показатель «среднее время наработки на опасное событие» (Mean Time To Hazardous Event = MTTHE), что не оказало бы никакого влияния на процесс.

2.4 Режимы работы

В стандарте EN 50129 режим «малой нагрузки» («низкого спроса» = low demand) не используется во избежание возникновения неоднозначности. Различие между режимами работы является искусственным:

- Целью комплекса мер по обеспечению безопасности системы является устранение или, при невозможности такового, обеспечение контроля за отказами.
- В программируемых электронных системах (ПЭС = PES, programmable electronic systems) это обычно означает уменьшение частоты возникновения опасных событий.
- Частота относится к непрерывному промежутку времени, так что представляется естественным, что для этого требуется работа системы в непрерывном (continuous) режиме.
- Использование в качестве целевого показателя вероятности отказа в выполнении запроса на обслуживание (Probability of Failure on Demand = PFD) обычно требует определения интервала проверок, обеспечивающего надежность (proof test interval), который задается оператором (т. е. эксплуатирующей организацией), а не поставщиком системы. Для поставщика более естественным является выполнять целевые показатели, заданные в форме уровней угроз (hazard rates), а не в форме PFD.
- Возможно установление соотношения между PFD и значениями частоты возникновения опасных событий (и наоборот).

На ряде примеров [17] показано также, что, в зависимости от того, какой режим работы выбран лицом, производящим анализ, один и тот же количественный анализ рисков приводит к разным значениям уровня целостности безопасности (SIL). Этот факт является внутренним

противоречием со стандартом IEC 61508!. Такая концепция стандарта EN 50129 эквивалентна новому подходу [18], в настоящее время изучаемому МЭК (IEC).

2.5 Доказательства соответствия требованиям безопасности (Safety Cases)

В стандарте IEC 61508 эта важная тема ясно не освещена. В этой области на стороне CENELEC имеются все преимущества стандартов, ориентированных на отрасль:

- четкая структура доказательства соответствия требованиям безопасности (Safety Case);
- соображения по доказательству соответствия требованиям безопасности (Safety Case) при перекрестной приемке (Cross-Acceptance) с привязкой к структурированному стандартизированному жизненному циклу (life cycle) и использованием гармонизованного набора документации;
- поддержка повторного использования и принципа модульности путем определения различных видов сертификации: для изделий общего применения, для приложений общего применения и для конкретных применений;
- четкие требования в части независимости разработчика, верификатора (verifier= проверяющий.), контролера (validator: лицо, назначенное для проведения проверки соответствия требованиям = validation) и эксперта (assessor = лицо, проводящее экспертизу или оценку).

2.6 Заключение

Концепции, положенные в основу стандартов IEC 61508 и EN 50126/EN 50129, совместимы. Они совпадают в следующем:

- подход на основе риска;
- концепция жизненного цикла безопасности;
- подход с учетом задания целевых показателей безопасности и
- определение уровня целостности безопасности (SIL).
- Различия между указанными стандартами следующие:
- уровень детализации системы (стандарты EN 50126/EN 50129 являются более общими);
- использование понятия режимов работы (стандарты EN 50126/EN 50129 являются более ограничивающими);
- интеграция обобщенного показателя RAM и безопасности (в стандарте IEC 61508 рассматривается только безопасность);
- степень подробности (например, руководящие указания для определения уровня целостности безопасности SIL);
- концепция доказательства соответствия требованиям безопасности (Safety Case): не содержится в явной форме в стандарте IEC 61508 и

- терминология.

3. Взаимосвязь с германскими руководящими указаниями

3.1 Руководящие указания Mü 8004

Традиционные руководящие указания Германских железных дорог Mü 8004 для магистральных линий представляют подход к безопасности на основе правил. Для каждого вида приложения, связанного с безопасностью, установлен определенный набор правил проектирования и, коротко говоря, если конкретным изделием эти правила выполняются, данное изделие считается удовлетворяющим требованиям безопасности и может быть допущено к применению в Германии. Такой порядок более конструктивен, чем подход CENELEC, но в то же время он обладает недостатками в части введения новых технологий (для которых еще не существует правил) и в части конкуренции, поскольку руководящие указания Mü 8004 подразумевают определенные архитектуры безопасности, а применение других вариантов не разрешается.

Другое серьезное различие между руководящими указаниями Mü 8004 и стандартами CENELEC состоит в том, что определение безопасности в Mü 8004 не основано на риске. Поэтому не было возможности непосредственно присвоить руководящим указаниям Mü 8004 статус международного стандарта. Принципиально философия, положенная в основу руководящих указаний Mü 8004, представляет собой стратегию «снизу - вверх», основанную на опыте: безопасные системы строятся из набора безопасных компонентов.

Подход, принятый в руководящих указаниях Mü 8004, имеет много преимуществ, которые, где возможно, были заимствованы из него в стандарты CENELEC, например, структура и содержание доказательства соответствия требованиям безопасности (Safety Case) или качественные правила обеспечения независимости элементов.

3.2 Руководящие указания VDV 331

В другом сборнике руководящих указаний по сигнализации на линиях региональных (пригородных) железных дорог и метрополитенов - VDV 331 [19] - уже используется подход к безопасности, основанный на риске, для чего применяется график (диаграмма) риска, представляющий собой в основном качественный метод анализа риска. График (диаграмма) риска явно упомянут в стандарте IEC 61508 как пример метода. Критерий допустимости риска непосредственно не выражен, но включен в график (диаграмму) риска. Это и явилось основной причиной, почему график (диаграмма) риска, несмотря на ряд привлекательных свойств, не смог стать стандартным методом в стандарте EN 50129. Не вполне ясно и то, каковы взаимосвязи между графиком (диаграммой) риска и другими критериями допустимости риска, например, GAMAB (globalement au moins aussi bon = в целом по меньшей мере также хорошо) или ALARP (as low as reasonably practicable = так низкий, как это практически возможно).

Поскольку документ VDV 331 соответствует стандарту IEC 61508, он соответствует и стандартам CENELEC. Практическая структура такого соответствия приведена на *рис. 3*. В документе VDV 331 график (диаграмма) риска используется для присвоения функциям значений уровней целостности безопасности (SIL). Отказы этих функций сразу же вызывают возникновение угроз, и соответствующие значения THR = TFM могут быть определены по таблице уровней целостности безопасности (SIL) стандарта IEC 61508 (или EN 50129).

Необходимо, однако, разъяснить, что успешное применение графика (диаграммы) риска зависит от четкости определения качественных параметров (строгость (Severity = S), время воздействия и частота (Exposure and Frequency = A), снижение риска (Risk Reduction = G) и вероятность возникновения события (Probabliity of Occurrence = W на *рис. 3*), а также от знаний и опыта аналитика в прикладной области. Хотя документ VDV 331 и содержит удовлетворительные определения и руководящие указания для линий региональных (пригородных) железных дорог и метрополитенов, возможность осмысленного перенесения этого подхода на магистральные линии железных дорог пока еще не продемонстрирована.

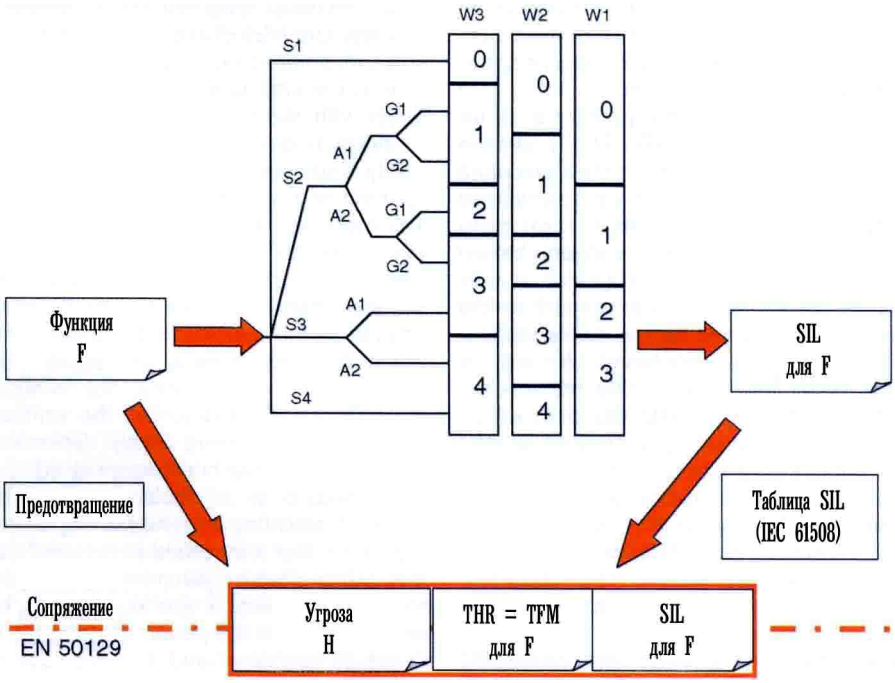

Рис. 3. Процедура задания целевых показателей безопасности с помощью графика (диаграммы) риска

4. Взаимосвязь с японскими руководящими документами по безопасности

Хотя в Японии руководящие документы по безопасности при введении микроэлектроники в железнодорожную сигнализацию были разработаны в 1980-е годы после комиссионной приемки первой японской микрокомпьютерной системы централизации, они являются внутриведомственными документами. Чтобы удовлетворить более высокие требования к безопасности системы и обеспечить выполнение более сложных функций, в 1996 г. комитетом специалистов при секретариате НИИ железнодорожной техники (Railway Technical Research Institute = RTRI) были

составлены новые руководящие указания по безопасности. До настоящего времени руководящие указания по безопасности применяются полностью или частично к некоторым новым системам сигнализации, включая модификации систем.

Основные характеристики новых руководящих указаний по безопасности следующие:

- Руководящие указания, составленные на основе стандарта IEC 61508, содержат необходимые технические условия, выработанные за длительный период создания и эксплуатации систем железнодорожной сигнализации в Японии.
- Руководящие указания содержат необходимые условия для управления безопасностью и технических мероприятий в течение жизненного цикла и не предназначены для применения в качестве правил.

Руководящие указания состоят из семи глав. Область применения и определения рассмотрены в первых двух главах. Принципы обеспечения безопасности на основе понятия безопасности при отказах (fail-safety) и концепций управления безопасностью и соответствующих мероприятий в течение жизненного цикла рассмотрены в главах 3 и 4. Глава 5 содержит определение жизненного цикла безопасности и технические требования к каждому процессу, входящему в жизненный цикл. Оценка безопасности и документация описаны в двух последующих главах. Более подробное обсуждение приведено в работе [20].

При разработке как японских руководящих указаний по безопасности, так и европейских стандартов (EN) были в принципе использованы концепции стандарта IEC 61508, но все же между ними имеется ряд различий. Основное различие заключается в том, что, тогда. как европейские стандарты (EN) предназначены для использования в качестве юридических документов (обязательных правил), японские руководящие указания по безопасности лишь рекомендовано принять. Другое существенное различие можно увидеть в том, что руководящие указания состоят из трех уровней - основного текста, пояснений и информации и интегрируют программное обеспечение, передачу информации и системы. Основной текст содержит описание главных понятий руководящих указаний, а подробности и конкретные идеи даны на уровне пояснений. Пояснения дополняются информацией (справочными сведениями).

В дополнение к указанному выше следует сказать, что методы количественного анализа, предписываемые в основном стандартом EN 50129, все еще являются предметом обсуждения. В приложении A, в котором рассматривается концепция уровня целостности безопасности (SIL), имеется таблица, в которой заданы количественные значения уровней целостности безопасности, например, менее, чем 10^{-9}/час для уровня SIL 4. В Японии существует ощущение, что количественный анализ следует применять только для целей выявления наиболее критичной части и подтверждения результатов применения последовательного подхода к обеспечению безопасности.

Путем присвоения численных значений каждому виду угрозы действительно становится возможным выявить более опасные точки и принять в их отношении необходимые меры. Для этого, однако, абсолютные значения не являются безусловно необходимыми, и вполне достаточно относительных значений. Таким образом, абсолютные значения не следует рассматривать как

целевые при принятии решения по выбору дальнейшего процесса обеспечения безопасности. Количественные значения следует использовать на сравнительно позднем этапе для подтверждения соответствия требованиям результатов каждого последующего этапа процесса обеспечения безопасности. Анализу рисков, выявляющему причины отказов, следует уделить большее внимание, чем количественному анализу рисков, в связи с недостаточностью данных и с применением принципа безопасности при отказах (fail-safe principle).

Другим важным аспектом, который должен быть принят во внимание, являются организационные и юридические вопросы. В стандарте EN 50129 изложен порядок приемки и сертификации по безопасности, и это глубоко связано с организацией или системами права каждой страны. Хотя этот стандарт тщательно проработан с учетом некоторых приспособлений к условиям конкретных стран, мы все же должны понять, имеются ли в нем какие-либо неудобства в части применения его в других странах, в особенности вне Европы.

5. Взаимосвязь с стандартами США

В настоящее время в США нет ни единого стандарта или правил по обеспечению безопасности, ни набора таких стандартов или правил для систем, основанных на применении процессоров, аналогичных европейским стандартам EN 50126, EN 50128 [2] и EN 50129. Скорее можно сказать, что в США обычной практикой для поставщиков стало создание своих собственных и часто уникальных процедур обеспечения безопасности на основе ряда различных стандартов, разработанных разными организациями. Главной причиной этого стало то, что различные существующие стандарты не охватывают всех ключевых аспектов обеспечения безопасности для критичных по безопасности изделий и систем железнодорожного назначения, или же вообще не содержат их, или же содержат, но с недостаточной степенью строгости. В связи с недостаточностью регулирования в этой области поставщики кладут в основу своих процедур такие стандарты, как «Сборник практических рекомендаций по связи и сигнализации» AREMA (American Railway Engineering and Maintenance-of-Way Association = Американская ассоциация по технике железнодорожного транспорта и техническому обслуживанию пути) [21], военный стандарт MIL-STD-882C на безопасные программы и анализ угроз, сравнительно недавно изданный институтом IEEE (Institute of Electrical and Electronics Engineers = Институт инженеров по электротехнике и электронике) стандарт IEEE 1483-2000 [22] по верификации безопасности, стандарт IEEE 1012-1998 [23] на процедуры верификации (verification) и проверки соответствия требованиям (validation) (процедуры «V&V») программного обеспечения, а также отдельные части прочих стандартов из других отраслей.

Для того, чтобы принять во внимание требования безопасности в свете технологического прогресса с учетом использования систем на основе процессоров в критичных по безопасности применениях на железнодорожном транспорте, Федеральная железнодорожная администрация США (Federal Railroad Administration = FRA) несколько лет назад начала работу по пересмотру существующих правил. Результатом этой работы явились создание Консультативного комитета по безопасности на железнодорожном транспорте

(Railroad Safety Advisory Committee = RSAC) и разработка и недавняя публикация в Кодексе Федеральных Правил (Code of Federal Regulations = CFR) Уведомления о предлагаемых руководящих указаниях (правилах) (Notice of Proposed Rulemaking = NPRM) [24]. Хотя придание этой публикации или какой-либо ее последующей редакции статуса действующих правил до конца 2003 года не ожидается, она содержит относительно полный набор требований к обеспечению безопасности систем на основе процессоров.

В свете вышеуказанного в приведенном ниже обсуждении основное внимание уделяется различным стандартам, используемым в США наиболее широко.

5.1 Стандарт MIL-STD-882

Стандарт MIL-STD-882 «Требования к программам обеспечения безопасности» («System Safety Program Requirements»), хотя и является стандартом Министерства обороны США, используется и как действующий стандарт в отрасли железнодорожного транспорта для разработки планов-программ обеспечения безопасности систем (System Safety Program Plans = SSPP). Такие планы, разрабатываемые поставщиками для конкретного изделия или применения, описывают процесс (комплекс мероприятий) обеспечения безопасности системы, подлежащий реализации. План SSPP охватывает все технические и управленческие мероприятия, которые должны быть осуществлены с целью обеспечения и демонстрации безопасности изделия или системы. Типичные мероприятия, подробно изложенные в плане SSPP, включают следующие:

- управление безопасностью, охватывающее организационные и прочие аспекты, обеспечивающие соответствие программе безопасности;
- анализ угроз и связанную с ним оценку рисков с целью выявления и оценки угроз и относящихся к ним рисков, а также
- процедуру верификации и оценки соответствия требованиям (Verification & Validation = V&V) для демонстрации уровня безопасности.

Планы-программы обеспечения безопасности систем (SSPP) обычно разрабатываются на основе внутренней процедуры обеспечения безопасности, принятой на предприятии-поставщике, и требований заказчика. Это означает, что обычно у поставщика имеется документированный процесс (включая процедуры) обеспечения безопасности, охватывающий технические и относящиеся к управлению мероприятия по обеспечению безопасности, подлежащие выполнению для всех жизненно важных изделий, который при разработке плана SSPP приспосабливается к конкретному изделию или применению для конкретного заказчика.

Стандарт MIL-STD-882, как и стандарты EN 50126/EN 50129, относится к жизненному циклу системы, но охватывает только безопасность, но не надежность, пригодность к техническому обслуживанию (ремонтопригодность) или же качество. Стандарт MIL-STD-882 не содержит точно определенной программы обеспечения безопасности, точно заданного перечня мероприятий, точно заданной процедуры доказательства соответствия требованиям безопасности (Safety Case) или же перечня соответствующей документации, а, скорее, рассчитан на приспособление к конкретной программе разработки.

Кроме того, что стандарт MIL-STD-882 является первичной основой для программ обеспечения безопасности, он также является действующим промышленным стандартом на проведение различных видов анализа угроз, в том числе предварительного анализа угроз, анализа угроз для подсистем и анализа угроз для эксплуатации и технического обслуживания. Как таковой, этот стандарт весьма подобен стандарту EN 50129 в части охватываемых им аспектов управления безопасностью.

Как и стандарты EN 50126/EN 50129, стандарт MIL-STD-882 основан на рисках, но, в отличие от них, не основан на уровнях целостности безопасности (SIL). Все же в стандарте MIL-STD-882 заданы категории управления программным обеспечением, что дает возможность охватить им вероятностные аспекты угроз, связанных с программным обеспечением, но эти категории не имеют того же назначения, что уровни целостности безопасности (SIL) в стандартах CENELEC. Действительно, за исключением нескольких уровней целостности для программного обеспечения, содержащихся в документах IEEE (рассмотренных ниже в настоящей статье), уровни целостности безопасности (SIL) на железнодорожном транспорте США не применяются. Определения степени тяжести (severity = «суровость») и вероятности угрозы в стандарте MIL-STD-882 весьма подобны таковым в стандарте EN 50126, но некоторые небольшие различия все же имеются. Стандарт MIL-STD-882, например, содержит пять категорий вероятности угроз, а стандарт CENELEC - шесть.

Категория «случайная» (occasional) в стандарте EN 50126 не соответствует категории «случайная» (occasional) в стандарте MIL-STD-882. Аналогично, определение категории «критичная» (critical) в стандарте MIL-STD-882 отличается от соответствующего определения в стандарте EN 50126. В стандарте EN 50126 имеется определения «одиночная фатальность» (single fatality), в то время как в стандарте MIL-STD-882 его нет.

Стандарт MIL-STD-882 является в значительной степени более наглядным, чем стандарты EN 50126/EN 50129, в части видов и содержания анализа угроз, но значительно менее наглядным, чем стандарт EN 50129, в части процедуры верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V).

Используются два основных варианта стандарта MIL-STD-882: вариант C и вариант D. Вариант MIL-STD-882C от 19 января 1993 г. является значительно более наглядным, чем вариант MIL-STD-882D от 10 февраля 2000 г., и поэтому используется более широко, чем вариант D.

5.2 Стандарт IEEE 1483 на верификацию безопасности

Институтом IEEE (Institute of Electrical and Electronics Engineers = Институт инженеров по электротехнике и электронике) недавно утвержден стандарт IEEE 1483-2000 (Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control = Стандарт на верификацию жизненно важных функций в процессорных системах, применяемых для управления на железнодорожном транспорте). Этот документ является результатом процесса достижения консенсуса в отрасли и не является официально обязательным, но в настоящее время широко используется на железнодорожном транспорте при проведении верификации безопасности систем и изделий, построенных на базе ЭВМ.

В стандарте описывается процесс, основой структуры которого являются три уровня верификации, осуществляемой аналитическими средствами:

- уровень концепций, охватывающий концепции обеспечения безопасности, иногда называемые принципами разработки (проектирования), факторы, от которых зависят эти концепции, и методы, необходимые для анализа концепций;
- функциональный уровень, на котором исчерпывающе выявляются жизненно важные функции, и
- уровень реализации, на котором производится проверка того, что жизненно важные функции реализованы с надлежащим уровнем безопасности, включая количественный анализ, а также, при возможности, качественный анализ на основе значения показателя MTTHE (Mean Time To Hazardous Event = «среднее время наработки на опасное событие»).

Процесс, описанный в стандарте IEEE 1483, определяет ряд аналитических операций, в том числе анализ дерева отказов, которые могут быть использованы для верификации, но принципиально оставляет определение конкретных видов анализа, подлежащих проведению на указанных трех уровнях, на усмотрение организации, выполняющей верификацию (или задающей требования для нее). Стандарт описывает мероприятия по верификации как в высокой степени зависящие от принятой архитектуры системы.

Стандарт как целое указывает виды мероприятий и сопровождающую документацию, необходимые для демонстрации того, что целевые показатели безопасности (требования) выполнены. Это делает его весьма подобным по своему характеру разделу стандарта EN 50129, относящемуся к демонстрации функциональной и технической безопасности (Evidence of Functional and Technical Safety). Стандарт IEEE 1483, например, требует описания концепций обеспечения безопасности, аналогичного по назначению описанию технических принципов, обеспечивающих безопасность разрабатываемого изделия, требуемому стандартом EN 50129.

Точно так же, стандарты EN 50126/EN 50129 описывают систематический подход к выбору подходящей (пригодной) архитектуры системы, а стандарт IEEE 1483 содержит информацию, оказывающую помощью при определении подходящих (пригодных) или допустимых системных архитектур. Одно небольшое различие в этой части состоит в том, что стандарт IEEE 1483 допускает одноканальную архитектуру, основанную на применении диагностики и самопроверки, а стандарт CENELEC - нет. Другое подобие между стандартами IEEE 1483 и EN 50129 заключается в том, что оба они в значительной мере оставляют на усмотрение соответствующих организаций выбор конкретных методов для применения.

Как и для стандарта EN 50129, разработка и процедура верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V) программного обеспечения являются предметом других документов: стандарта CENELEC EN 50128 в Европе и, соответственно стандарта IEEE 1012 и других стандартов IEEE в США.

Как стандарт EN 50129, так и стандарт IEEE 1483 устанавливают, что задание количественных целевых показателей безопасности и демонстрация их выполнения должны осуществляться соответствующим государственным органом или организацией. В стандарте EN 50129 в основу количественного целевого показателя безопасности положены случайные и систематические отказы (при этом требования, относящиеся к систематическим отказам, проверяются не количественно, а посредством уровней целостности безопасности - SIL), в то время как в стандарте IEEE 1483 количественный целевой показатель задан через параметр MTTHE. Части системы, дающие вклад в этот целевой показатель (например, аппаратура и программное обеспечение), в стандарте IEEE 1483 не заданы, хотя в этом стандарте и признается, что может оказаться необходимым определение количественных значений вероятности или частоты возникновения соответствующих факторов. В стандарте EN 50129 качественный целевой показатель безопасности определяется через уровень целостности безопасности (SIL), в то время как в стандарте IEEE 1483 качественный «целевой показатель» основан на демонстрации живучести функций, определенных как жизненно важные.

Имеется и ряд существенных различий между стандартами IEEE 1483 и EN 50129. В отличие от стандарта EN 50129, стандарт IEEE 1483 не основан на уровне целостности безопасности (SIL). Он основан на определении функций, являющихся жизненно важными, и верификации этих функций прежде всего аналитическими средствами. Как указывалось выше, на железнодорожном транспорте США уровень целостности безопасности (SIL) не применяется, хотя в гражданской авиации подобные понятия существуют. Кроме того, стандарт IEEE 1483 основное внимание уделяет верификации безопасности, но не содержит аспектов проверки соответствия требованиям (validation). Раздел стандарта EN 50129, относящийся к демонстрации функциональной и технической безопасности (Evidence of Functional and Technical Safety), содержит требования к квалификационным испытаниям по безопасности (Safety Qualification Testing), которые, вместе с другими аспектами проверки соответствия требованиям (validation), не содержатся в стандарте IEEE 1483.

Стандарт IEEE 1483, в отличие от стандарта EN 50129, не предписывает необходимости в привлечении независимого эксперта (assessor) по безопасности.

5.3 Сборник практических рекомендаций по связи и сигнализации AREMA

Раздел 17.3 «Recommended Safety Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications» («Рекомендуемая программа обеспечения безопасности для электронных и программно-управляемых изделий, применяемых в жизненно важных системах сигнализации») Руководства по связи и сигнализации (Communications and Signals (C&S) Manual), изданного организацией AREMA (American Railway Engineering and Maintenance-of-Way Association = Американская ассоциация по технике железнодорожного транспорта и техническому обслуживанию пути), посвящен вопросам безопасности процессорных систем. Этот раздел руководства, частичного или полного соответствия которому в ряде случаев требуют железные дороги Северной Америки, содержит мероприятия и

аспекты общей программы обеспечения безопасности для систем и аппаратуры с процессорным управлением.

Раздел 17 содержит соображения по разработке изделий, организационные и управленческие (административные) аспекты обеспечения безопасности, включая планы SSPP (см. выше), анализ угроз, идентификацию и распределение требований по безопасности, процедуру верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V), а также количественные оценки. Назначением стандарта является охват всех аспектов обеспечения безопасности, а не только их части, как в стандартах MIL-STD-882 (планы-программы SSPP и анализ угроз) или IEEE 1483 (верификация безопасности). Этот документ также не является официально обязательным, а скорее представляет собой набор практических рекомендаций для железных дорог в части систем и аппаратуры с процессорным управлением, предназначенных для критичных по безопасности применений.

Раздел 17.3 Руководства AREMA устанавливает необходимость осуществления управления безопасностью, управления качеством и процедуры верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V). Процедура верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V) в Руководстве AREMA аналогична по своему назначению разделу стандарта EN 50129, относящемуся к демонстрации функциональной и технической безопасности (Evidence of Functional and Technical Safety). Таким образом, этот раздел аналогичен стандарту EN 50129 в части необходимости рассмотрения каждого из указанных аспектов при доказательстве соответствия требованиям безопасности (Safety Case). Такое подобие относится и к условиям, при которых должна осуществляться демонстрация безопасности (нормальная работа, отказы, внешние влияния и т. д.).

Мероприятия, входящие в процесс обеспечения безопасности, описанный в Руководстве AREMA (раздел 17.3), в части верификации программного обеспечения аналогичны по своему назначению комбинации стандарта MIL-STD-882, ряда аспектов стандарта IEEE 1483 и ряда аспектов стандарта IEEE 1012. Во многих отношениях они аналогичны по своему назначению и стандартам EN 50126, EN 50128 и EN 50129. Руководство AREMA, однако, в отличие от стандартов CENELEC, не основано на понятии уровня целостности безопасности (SIL), а также не является столь же наглядным и подробным, как эти стандарты, особенно в части демонстрации безопасности программного обеспечения. Аспекты Руководства AREMA, относящиеся к программному обеспечению, касаются только процедуры верификации и оценки соответствия требованиям безопасности (Verification & Validation = V&V), но не касаются более широких вопросов разработки программного обеспечения, рассмотренных в стандарте EN 50128.

В Руководстве AREMA, как и в стандарте EN 50129, указывается, что требования по безопасности должны включать качественные и количественные аспекты.

Раздел 17 Руководства AREMA содержит практические рекомендации и минимальные требования к обеспечению безопасности, надежности, пригодности к техническому обслуживанию (ремонтопригодности), а также к обеспечению качества. В этом смысле раздел 17 Руководства AREMA из всех

соответствующих американских документов оказывается ближе всего к стандарту EN 50126 в части установления интегрального подхода к безопасности, надежности, пригодности к техническому обслуживанию (ремонтопригодности) и качеству. Оперативная готовность (доступность = availability) не рассматривается в Руководстве AREMA так непосредственно, как в стандарте EN 50126, зато в Руководстве AREMA пригодность к техническому обслуживанию (ремонтопригодность = maintainability) рассматривается в некоторой степени через аспекты надежности и пригодности к техническому обслуживанию (ремонтопригодности = maintainability). Стандарт EN 50126 дает совместное определение безопасности, надежности, пригодности к техническому обслуживанию, оперативной готовности и качества как «обобщенной надежности» (dependability); понятие «обобщенная надежность» (dependability) не рассматривается таким образом ни в Руководстве AREMA, ни вообще в США.

Согласно Руководству AREMA, система обеспечения качества может быть основана на стандарте IEEE (IEEE 730.1-1995) [25] или на серии стандартов ISO. В части качества CENELEC также устанавливает требование соответствия стандарту ISO 9001 [26].

5.4 Стандарты безопасности RSAC

Консультативный комитет по безопасности на железнодорожном транспорте (Railroad Safety Advisory Committee = RSAC) был создан Федеральной железнодорожной администрацией США (Federal Railroad Administration = FRA) в 1996 г., в частности, с целью подготовки возможного пересмотра правил (частей 209, 234 и 236 раздела 49 Кодекса Федеральных Правил = Code of Federal Regulations, CFR), относящихся к новым программно-управляемым системам управления движением поездов. В течение 1990-х г.г. внутри комитета RSAC была организована рабочая группа по стандартам (Standards Task Force) для разработки правил в части систем безусловного (непосредственно воздействующего на движение поезда) управления движением поездов (Positive Train Control = PTC). Такие системы должны выполнять три основных функции:

- предотвращение столкновений поездов друг с другом;
- принудительное соблюдение ограничений скорости и
- обеспечение безопасности персонала, работающего на путях, и используемого им оборудования.

Для выработки консенсуса по предлагаемому пересмотру правил были созданы четыре группы, включающие представителей от Федерального Правительства, руководства железных дорог, работников железных дорог и поставщиков оборудования железнодорожной сигнализации и управления движением поездов.

В течение последних нескольких лет рабочей группой по стандартам на системы безусловного (непосредственно воздействующего на движение поезда) управления движением поездов (PTC Standards Task Force) выпущено и пересмотрено несколько проектов Уведомлений о предлагаемых руководящих указаниях (правилах) (Notice of Proposed Rulemaking = NPRM). 10 августа 2001 г. Федеральной железнодорожной администрацией США (Federal

Railroad Administration = FRA) был опубликован в Федеральном Реестре (Federal Register) проект правил («Предлагаемые Правила» = Proposed Rule) «Стандарты на разработку и использование систем сигнализации и управления движением поездов на базе процессоров» (Standards for the Development and Use of Processor-Based Signal and Train Control Systems). Этот проект правил в настоящее время не является обязательным официальным документом для железных дорог США, но весьма вероятно, что в 2003 г. этот документ или его какая-либо последующая редакция станет таковым.

Две ключевых темы Подраздела H данного проекта правил (NPRM) относятся к разработке планов-программ обеспечения безопасности на железнодорожном транспорте (Railroad Safety Program Plan = RSPP) и планов обеспечения безопасности изделий (Product Safety Plan = PSP). План RSPP является официальным документом, подлежащим разработке железными дорогами, который должен служить основным документом по безопасности для всех критичных по безопасности изделий, применяемых на железных дорогах. Назначение плана RSPP состоит в том, чтобы установить стратегию железных дорог в части угроз безопасности, связанных с эксплуатацией изделий, на которые распространяется действие Подраздела H документа CFR 236, а также задать минимальные требования к разработке и реализации таких изделий. Каждая железная дорога должна подать в Федеральную железнодорожную администрацию США (FRA) ходатайство об утверждении своего плана-программы обеспечения безопасности (RSPP).

Другой ключевой темой проекта правил (NPRM) является план обеспечения безопасности изделий (Product Safety Plan = PSP). Этот план должен являться официальным документом, детально описывающим все аспекты безопасности изделия, включая процедуры его разработки, реализации, монтажа, эксплуатации, технического обслуживания, ремонта, контроля, испытаний и внесения изменений (модификации), и содержащим анализ, подтверждающий заявленные показатели безопасности. Ожидается, что железные дороги будут обращаться к поставщикам изделий для предоставления большей части информации, необходимой для плана PSP. План PSP также будет подлежать утверждению в Федеральной железнодорожной администрации США (FRA).

Подраздел H определяет следующие 20 пунктов, которые, скорее всего, будет необходимо включать в план PSP:

- описание изделия;
- описание эксплуатационного процесса или категорий эксплуатационных процессов железной дороги, для которых будет использоваться данное изделие;
- документ об эксплуатационных концепциях - функции и потоки информации;
- документ о требованиях безопасности - описание всех функций, связанных с безопасностью;
- информацию о том, каким образом архитектура изделия удовлетворяет требованиям безопасности;
- сводка угроз, описывающая все угрозы, относящиеся к безопасности;

- оценка риска - расчет количественного значения уровня безопасности новой системы и системы, заменяемой ею;
- анализ путей снижения угроз;
- описание используемых процессов оценки безопасности и процедуры верификации и проверки соответствия требованиям (validation) (процедуры «V&V») и их результатов;
- описание анализа угроз;
- анализ человеческого фактора (при необходимости);
- описание обучения, необходимого для осуществления контроля, испытаний и технического обслуживания;
- описание конкретных процедур и испытательного оборудования для монтажа, эксплуатации, технического обслуживания и т. д.;
- описание необходимых мер безопасности (security - административной или безопасности информации, а не движения!);
- описание предупреждений по безопасности, которые должны быть включены в инструкции по эксплуатации и техническому обслуживанию;
- описание процедур обеспечения безопасности при монтаже;
- описание мероприятий по обеспечению безопасной эксплуатации в течение жизненного цикла, включая ведение эксплуатационного журнала; и
- описание способов резервирования и критичных по безопасности предположений в части влияний на доступность (оперативную готовность), возможностей задания конфигурации изделия для различных применений и планируемого внесения изменений в новые версии.

В разделе 234 проекта NPRM рассматривается возможность применения требований Подраздела H к системам железнодорожной переездной сигнализации. Коротко говоря, системы переездной сигнализации, основанные на «новой или прогрессивной технологии», ранее не признававшейся допустимой для применения до даты утверждения настоящих правил, или же системы, выдающие критичные по безопасности данные в систему железнодорожной сигнализации, должны соответствовать требованиям Подраздела H части 236.

Проект NPRM определяет основанный на качестве работы (performance-based), не являющийся предписанием (не ограничивающий разработчиков), нейтральный по отношению к технологии стандарт для разработки и применения процессорных систем под юридическим контролем Федеральной железнодорожной администрации США (FRA). Указанные 20 пунктов плана PSP определяют объем доказательства соответствия требованиям безопасности (Safety Case) для конкретного изделия или системы. Доказательство соответствия требованиям безопасности (Safety Case) включает анализ и прослеживание угроз, процедуру верификации и проверки соответствия требованиям безопасности (validation) (процедуру «V&V»), оценку рисков, а также прочие указанные выше многочисленные пункты, относящиеся к разработке и демонстрации безопасности. План PSP охватывает аспекты

управления безопасностью, а также технические и функциональные аспекты безопасности, что делает его аналогичным разделам «Управление безопасностью» (Safety Management) и «Демонстрация функциональной и технической безопасности» (Evidence of Functional and Technical Safety) стандарта EN 50129. Аспекты обеспечения качества в план PSP в отличие от стандарта EN 50129 не входят. План PSP похож на стандарт EN 50129 также и тем, что в нем задается систематический подход к идентификации (выявлению) угроз, оценке путей снижения угроз и оценке рисков.

Проект NPRM содержит перечень стандартов, которые могут использоваться для задания требований к процедуре верификации и проверки соответствия требованиям безопасности (validation) (процедуре «V&V»), а также других требований, в особенности для плана PSP. Следует отметить, что этот перечень включает стандарты EN 50126, EN 50128 и EN 50129, а также IEC 61508, MIL-STD-882C, IEEE 1483 и Руководство AREMA. При использовании одного или нескольких из этих стандартов для задания требований по различным аспектам, требуемым проектом NPRM (план PSP), важным моментом является то, что применяемый метод должен соответствовать конкретному требованию в виде, изложенном в проекте NPRM. Применительно к процедуре верификации и проверки соответствия требованиям безопасности (validation) (процедуре «V&V») проект NPRM требует демонстрации безопасности при различных условиях, в том числе при нормальной эксплуатации, случайных отказах, систематических отказах и наличии внешних влияний, аналогично требованиям стандарта EN 50129.

Ключевым аспектом плана PSP, связанным с характером данного стандарта, основанного на качестве работы (performance-based), является необходимость оценки риска. Назначение оценки риска состоит в использовании ее для демонстрации с высокой степенью доверительности, что проверяемая система не вызовет риска, превосходящего предшествующее состояние. Это означает, что необходимы две оценки: одна для исходной (базовой) системы (при возможности), и другая - для новой системы, заменяющей ее. Оценка рисков основана в большей степени на относительном, а не на абсолютном риске. Хотя в проекте NPRM предпочтение отдается количественной оценке риска на основе показателя MTTHE или эквивалентного ему, он также допускает количественные и качественные оценки и их сочетание. В проекте NPRM не задан конкретный абсолютный количественный целевой показатель безопасности. Такой подход несколько отличается от требований стандартов EN 50126/50129, где прежде всего задан количественный целевой показатель безопасности, а затем - качественные целевые показатели на основе уровней целостности безопасности (SIL).

В проекте NPRM задано, что количественные оценки должны включать вклад человеческого фактора (при возможности) и прочих систематических отказов, таких, как ошибки программного кода. Этим он отличается от стандартов EN 50126/50129, в соответствии с которыми расчет количественного показателя безопасности не включает таких факторов, а основан исключительно на случайных (аппаратных) отказах.

Еще одно сходство между проектом NPRM и стандартами CENELEC заключается в том, что оба они требуют проведения оценки третьими лицами, а окончательная сертификация основана частично на результатах этих оценок. К настоящему времени такие оценки третьими лицами стали обязательными в

Европе, но не являются обязательными в США, хотя и проводятся в этой стране все более регулярно.

5.5 Стандарт IEEE 1012

Стандарт IEEE 1012-1998 «Стандарт на верификацию и оценку соответствия требованиям (Validation) программного обеспечения» (Standard for Software Verification and Validation) является стандартом, наиболее часто используемым в США для проведения процедуры верификации и проверки соответствия требованиям безопасности (validation) (процедуры «V&V») программного обеспечения. Он определяет логический и структурированный подход к выполнению различных видов анализа и проверок на разных этапах разработки программного обеспечения. На железнодорожном транспорте использование такого процесса, как этот, в связи со сложностью программного обеспечения оказывается необходимым почти всегда. Стандарт IEEE 1012 не является собственно стандартом по безопасности, но его применение всегда способствует устранению потенциально опасных ошибок в программном обеспечении, которые в ином случае могли бы остаться невыявленными. В процессе обеспечения безопасности этот метод проведения процедуры верификации и проверки соответствия требованиям безопасности (validation) (процедуры «V&V») программного обеспечения обычно применяется в сочетании с анализом угроз и другими видами анализа, связанными с безопасностью.

Стандарт IEEE 1012 определяет мероприятия, составляющие процедуру верификации и проверки соответствия требованиям безопасности (validation) (процедуру «V&V»), методы и документацию для четырех уровней целостности программного обеспечения (software integrity levels), а также различные этапы разработки программного обеспечения. Уровни целостности программного обеспечения в стандарте IEEE 1012 основаны на критичности программного обеспечения, которая может включать безопасность (safety), защиту информации (security), сложность программного обеспечения, качество работы (performance), надежность и другие факторы. Эти уровни чем-то подобны пяти уровням целостности программного обеспечения, определенным в стандарте EN 50128. Первые четыре уровня целостности программного обеспечения в стандарте EN 50128 относятся к критичному по безопасности программному обеспечению, в стандарте же IEEE 1012 этого нет. Таким образом, стандарт EN 50128 более конкретно нацелен на безопасность программного обеспечения. В стандарте IEEE 1012 безопасность является, однако, одним из факторов, которые могут вести к наивысшему уровню целостности программного обеспечения. Например, наивысший уровень целостности программного обеспечения в стандарте IEEE 1012 относится к программному обеспечению, которое потенциально может стать причиной катастрофических последствий с разной степенью вероятности. Существует много аналогий в части мероприятий, методов и документации, установленных стандартами IEEE 1012 и EN 50128 для разных этапов.

Стандарт IEEE 1012 устанавливает требования к плану процедуры верификации и проверки соответствия требованиям безопасности (validation) (процедуры «V&V») программного обеспечения аналогично стандарту EN 50128. Самое большое отличие состоит, однако, в том, что стандарт EN 50128 имеет более широкое назначение - он охватывает разработку программного

обеспечения, включая процедуру его верификации и проверки соответствия требованиям безопасности (validation) (процедуру «V&V»), в то время как стандарт IEEE 1012 сосредоточен исключительно на процедуре верификации и проверки соответствия требованиям безопасности (validation) (процедуры «V&V») программного обеспечения. Существует большое число и других стандартов IEEE, относящихся к различным другим аспектам разработки программного обеспечения.

Литература

1. CENELEC, EN 50126. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1998. To be published as IEC 62278 (Применения на ж.-д. транспорте. Спецификация и демонстрация надежности, доступности, ремонтопригодности и безопасности. Подлежит опубликованию как стандарт IEC 62278).
2. CENELEC, EN 50128. Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems. 2000. To be published as IEC 62279 (Применения на ж.-д. транспорте. Системы связи, сигнализации и обработки данных. Подлежит опубликованию как стандарт IEC 62279).
3. CENELEC, EN 50129. Railway applications - Safety-related electronic systems for signalling. 2002. To be published as IEC 6228x (Электронные системы сигнализации, связанные с обеспечением безопасности - применения на железнодорожном транспорте. Подлежит опубликованию как стандарт IEC 6228x).
4. CENELEC, EN 50159-1/-2. Railway applications - Communication, signalling and processing systems - Safety-related communication in open/closed communication systems. 2001. To be published as IEC 62280 (Применения на ж.-д. транспорте. Системы связи, сигнализации и обработки данных. Передача информации, связанной с безопасностью, в открытых/закрытых системах связи. Подлежит опубликованию как стандарт IEC 62280).
5. Luedeke, J. Safety of High-Speed Ground Transportation Systems, Analytical Methodology for Safety Validation of Computer Controlled Subsystems; Volume I: State-of-the-Art and Assessment of Safety Verification/Validation Methodologies, DOT -VNTSC-FRA-95-8.1; Volume II Development of a Safety Validation Methodology, DOT-VNTSC-FRA-95-8.11,1995 (Безопасность высокоскоростных наземных транспортных систем. Методология анализа для оценки соответствия требованиям безопасности подсистем, управляемых от ЭВМ. Том 1: Современное состояние и оценка методологий верификации и оценки соответствия требованиям (Validation); том 2: Разработка методологии оценки соответствия требованиям безопасности).
6. IEC 65A(Sec)122: Software for computers in the application of industrial safety-related systems. 1992 (Программное обеспечение для ЭВМ, применяемых в промышленных системах, связанных с обеспечением безопасности).

7. IEC 65A(Sec)123. Functional safety of electrical/electronic/programmable electronic safety-related systems; generic aspects; part 1: general requirements. 1993 (Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с обеспечением безопасности; общие аспекты; часть 1: общие требования).
8. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. 2000 (Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с обеспечением безопасности).
9. Federal German Railways Office (EBA), Mü 8004. Anweisung zu den technischen Anforderungen für die Zulassung von Sicherungsanlagen (Федеральное управление Германских железных дорог (EBA). Документ Mü 8004. Руководящие указания по техническим требованиям к сертификации систем обеспечения безопасности).
10. Ministry of Defence (UK), Def Stan 00-55: Requirements for Safety Related Software in Defence Equipment. 1997 (Министерство обороны Великобритании. Военный стандарт 00-55: Требования к программному обеспечению, связанному с обеспечением безопасности, для оборудования военного назначения).
11. Ministry of Defence (UK), Def Stan 00-56: Safety Management Requirements for Defence Systems. 1996 ((Министерство обороны Великобритании. Военный стандарт 00-56: Требования по управлению безопасностью для систем военного назначения).
12. Department of Defense (US), MIL-STD-882: System Safety Program Requirements. 1993 (version C), 2000 (version D) (Министерство обороны США: стандарт MIL-STD-882: Требования к программам обеспечения безопасности).
13. IEC 60300: Dependability Management. 1997 (Управление обобщенной надежностью).
14. Braband, J.: RAMS-Management nach CENELEC. SIGNAl+DRAHT, 1998, № 11 (Управление показателями надежности, оперативной готовности, пригодности к техническому обслуживанию и безопасности в соответствии со стандартами CENELEC).
15. Herrmann, D. Software Safety and Reliability - Techniques, Approaches and Standards of Key Industrial Sectors. IEEE Press, 1999 (Безопасность и надежность программного обеспечения - Методы, подходы и стандарты в ключевых отраслях промышленности).
16. Braband, J.; Reder, H.-J.: Sicherheitstechnische Vorgehensweise in der Eisenbahnsignaltechnik und Luftfahrt. SIGNAl+DRAHT, 2003, № 1+2 (Процедуры обеспечения безопасности в железнодорожной сигнализации и гражданской авиации).
17. Sundvall, K.-E.: Establishing Safety Integrity Level (SIL) from frequency of failure. Report SP 80085, 1998 (part of CENELEC report RO09-0042001) (Определение уровня целостности безопасности на основе частоты отказов. Отчет SP 80085, 1998 - часть отчета CENELEC RO09-0042001).

18. Kato, E; Sato, Y.: Safety Integrity Level Models for IEC 61508 - Examination of modes of operation. IEEE Trans. Fundamentals, vol. E83-A, 2000, 863 - 865 (Модели уровня целостности безопасности для стандарта IEC61508 - Исследование режимов работы. Труды IEEE по общенаучным вопросам, том E83-A, 2000, стр. 863 - 865).
19. VDV. Anforderungsklassen für Signal- und Zugsicherungsanlagen gemäß BOStrab (Классы требований к системам сигнализации и обеспечения безопасности движения поездов в соответствии с Положением о строительстве и эксплуатации городских железных дорог). VDV 331, 1994.
20. Hirao, Y.: New European Norms from a Japanese Viewpoint. SIGNAl+DRAHT, 2001, № 11 (Новые европейские стандарты с японской точки зрения).
21. American Railway Engineering and Maintenance-of-Way Association (AREMA): Communications and Signals Manual of Recommended Practices 2000 (Американская ассоциация по технике железнодорожного транспорта и техническому обслуживанию пути: Сборник практических рекомендаций по связи и сигнализации).
22. IEEE 1483-2000. Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control. March 30, 2000 (Стандарт на верификацию жизненно важных функций в процессорных системах, применяемых для управления на железнодорожном транспорте. 30 марта 2000 г.).
23. IEEE 1012-1998. Standard for Software Verification and Validation. IEEE Computer Society, July 20, 1998 (Стандарт на верификацию и оценку соответствия требованиям (Validation) программного обеспечения. Компьютерное общество IEEE, 20 июля 1998 г.).
24. Standards for the Development and Use of Processor-Based Signal and Train Control Systems; Proposed Rule. Federal Register, August 10, 2001 (Стандарты на разработку и использование систем сигнализации и управления движением поездов на базе процессоров. Предложение (проект) правил. Федеральный реестр США, 10 августа 2001 г.).
25. IEEE 730.1. Guide for software quality assurance planning. January 1, 1995 (Руководящие указания по планированию мер по обеспечению качества программного обеспечения. 1 января 1995 г.).
26. 150 9001. Quality management systems - Requirements. 2000 (Системы управления качеством - Требования).