Проект единой методологии оценки риска для обеспечения безопасности на железных дорогах Европы

Перед европейским железнодорожным агентством (European Railway Agency, ERA) стоит настоятельная задача определения общих целей в области безопасности и внедрения общей методологии управления безопасностью в Европе. Назначение настоящей статьи состоит в содействии формированию единой отраслевой точки зрения на обоснование требований по безопасности технических систем и на способы демонстрации их соответствия этим требованиям. В статье рассматривается проект, в котором интегрируются количественные и качественные подходы, поддерживается достигнутый уровень безопасности, вводится гармонизированный критерий приемлемости риска для технических систем на железных дорогах Европы и который является одновременно экономически эффективным и удобным в использовании. Основой проекта является передовой опыт, наработанный европейской железнодорожной промышленностью.

Миссия европейского железнодорожного агентства ERA, образованного в соответствии с постановлением ЕС 881/2004, заключается в укреплении безопасности и эксплуатационной совместимости железнодорожных сетей по всей Европе в период продолжающейся приватизации железных дорог. В соответствии с этой миссией усилия ERA сконцентрированы на разработке методологии, включающей постановку единых целей в области безопасности (common safety targets, CSTs), единые методы обеспечения безопасности (common safety methods, CSMs), единую систему показателей безопасности (common safety indicators, CSIs) и согласованные документы сертификации безопасности.

Едиными целями CSTs задаются минимальные уровни безопасности, выраженные в терминах допустимости риска, и показатели эффективности ее достижения, которые должны быть обеспечены в железнодорожной системе европейских государств как в едином целом.

Единые методы CSMs увязывают уровни безопасности, оценки достижения целей в области безопасности и оценки соответствия другим требованиям по безопасности, принятые в разных странах Европы.

Своей работой ERA стремится значительно расширить область применения существующих стандартов и руководств комитета CENELEC. В июне 2007 г. агентство ERA разослало проект предложений по единым методам обеспечения безопасности (CMS) для рецензирования заинтересованными кругами на железных дорогах. Предполагается, что этот проект получит статус постановления ЕС в апреле 2008 г.

Назначение настоящей статьи в том, чтобы показать поставщикам технических систем для железных дорог, как следует осуществлять декомпозицию требований по безопасности движения и как следует демонстрировать соответствие этим требованиям. В статье также излагается концепция обоснования требований по безопасности движения, которыми должны руководствоваться поставщики железнодорожных систем. Важно отметить, что эта концепция недавно была принята в качестве официальной позиции европейского союза предприятий железнодорожной промышленности UNIFE в отношении единых методов обеспечения безопасности CSM.

В настоящей статье термином «техническая система» обозначается продукция предприятий железнодорожной промышленности, включающая:

- проект системы,
- внедренную систему,
- сопроводительную документацию.

Директива ЕС по безопасности движения утверждает, что уровни безопасности на железных дорогах сообщества в целом высоки и что важно, чтобы в течение переходного периода поддерживалась, по крайней мере, такая же безопасность.

Для решения этой задачи на разных уровнях управления безопасностью вводятся измеримые цели. Прежде всего цели в области безопасности устанавливаются на уровне государств — членов ЕС. Агентство ERA уже предоставило примеры измеримых показателей для определения этих целей. В частности, по показателю «число несчастных случаев на миллион поездо-километров» агентством собрана и опубликована предварительная статистика. Железнодорожные предприятия, например операторы инфраструктуры, используют термин «уровень без-

Таблица 1

Краткий обзор терминологии

Термин	Системный уровень	Ответственность	Примечания
Цель в области безопасности	Вся железнодорожная система	Государства — члены ЕС	Определяется на основе статистических показателей, например «количество несчастных случаев на миллион поездо-километров»
Уровень безопасности	Функциональная подсистема	Железнодорожные предприятия, например операторы инфраструктуры, предприятия — перевозчики и т. д.	Содержит комплекс качественных и количественных показателей безопасности
Требования по безопасности	Техническая система	Промышленность систем и средств для железнодорожного транспорта	Содержит функциональные требования, требования к полноте безопасности

опасности», который, однако, еще не определен в директиве ЕС по безопасности движения. В настоящее время предлагается использовать термин «эффективность безопасности системы или подсистемы» («safety performance of a system or subsystem»), который, таким образом, представляет собой набор качественных и количественных показателей. Для характеристики безопасности обычно используется термин «требования по безопасности», который, однако, в последнее время стал употребляться агентством ERA в более узком контексте — применительно к техническим системам и средствам. В этом контексте термин означает совокупность качественных и количественных требований, т. е. функциональных требований и требований по полноте безопасности. Для предотвращения терминологических ошибок термины, используемые в настоящей статье, сведены в таблицу.

Статистика несчастных случаев и их расследование показывают, что значительными, если не самыми важными, причинами несчастных случаев являются ошибки людей в сочетании с плохой организацией работ и недостатками в культуре безопасности. Доля технических отказов для систем сигнализации и подобных систем падает в этой статистике до незначительного уровня (достоверные оценки опускают этот уровень значительно ниже 1%). Это показано как теоретическим, так и опытным путем.

Результаты европейского исследовательского проекта SAMNET указывают на непроизводительность раскручивания в железнодорожном секторе «внутриотраслевой бесконечно восходящей спирали безопасности». Международный технический комитет (ITC) института инженеров в области СЦБ (IRSE) поддерживает эту точку зрения и в своем заключении по данному вопросу утверждает, что проведение отдельного анализа риска для каждой внедряемой в стране системы увеличивает затраты, прибыль по которым не ожидается; существует возможность заметного сокращения затрат на основе новых подходов, предусматривающих универсальный анализ риска.

Предварительные условия

В соответствии с изложенными выше сведениями основу настоящей статьи составляют следующие общие положения. Безопасность должна рассматриваться как составная часть единой структуры, включающей промышленность технических систем и средств железнодорожного транспорта, операторов инфраструктуры и другие железнодорожные предприятия. Должен существовать баланс между риском, связанным с действующими техническими системами, и риском, обусловленным действием человеческого и организационного факторов при эксплуатации и обслуживании. Культура безопасности и системы управления являются важнейшими составляющими безопасности движения.

Единая структура должна опираться на уровни безопасности, уже достигнутые в технических системах. Необходимо сосредоточиться на их интеграции в составе новых железнодорожных систем, т. е. на процессах адаптации и инновации. Единая структура должна обеспечивать гармонизацию, а лучше — стандартизацию правил и процессов обеспечения безопасности движения во всей Европе для поддержания конкурентоспособности европейской железнодорожной отрасли.

Базовый процесс обоснования требований по безопасности

Исходными действиями по выполнению этого процесса являются определение назначения системы и идентификация связанных с нею угроз.

Далее идентификация угроз дополняется их классификацией, эти действия в совокупности хорошо известны как предварительный анализ угроз (preliminary hazard analysis, PHA). В результате этого анализа идентифицированные угрозы ранжируются по их критичности путем, например, присвоения им номеров, обозначающих приоритет связанного с этой угрозой риска. Если критичность угрозы оказывается ниже определенного порога, установленного полномочным органом по безопасности,

то угроза считается пренебрежимой и процесс анализа риска для нее не проводится. Тем самым дальнейшие усилия можно сконцентрировать на существенных угрозах. Единственное, что необходимо при этом еще сделать, — это провести независимую экспертизу критичности угроз.

Далее для каждой значительной угрозы предлагается следующая процедура анализа риска:

- если существуют имеющие силу нормативные документы (например, правила, стандарты или руководства), то они должны быть применены. Нормативная документация может содержать детерминированные и вероятностные, а также качественные и количественные требования. Управление соответствующей угрозой осуществляется на основе доказательства соответствия требованиям, установленным в нормативной документации;
- если для новой технической системы существует и доступна эталонная система, то должны быть приняты требования по безопасности для эталонной системы (если они существуют). Если требования по безопасности для эталонной системы не сформулированы, то в качестве таких требований принимаются значения показателей эффективности безопасности эталонной системы. Требования по безопасности могут быть выведены путем анализа эталонной системы, а также на основе рассмотрения записей, отражающих статистику управления безопасностью в этой системе. Управление угрозами при использовании такого подхода осуществляется предоставлением доказательств того, что в новой системе поддерживается уровень безопасности эталонной системы;
- если отсутствуют и действующие нормативные документы, и эталонная система (или существуют причины, по которым предыдущие варианты не могут быть применены), то должна быть выполнена явная оценка риска;

Структура этого процесса представлена на рис. 1. Конкретный метод (или методы) анализа риска должен быть выбран поставщиком на основе его опыта и знания системы.

Во всех случаях остаточные риски должны быть сопоставлены с критериями допустимости риска, которые могут быть как качественными, так и количественными. Для случая явной оценки риска в качестве эталонного значения следует использовать принятый железными дорогами Европы критерий допустимости риска для технических систем (RAC-TS — risk acceptance criterion for technical systems).

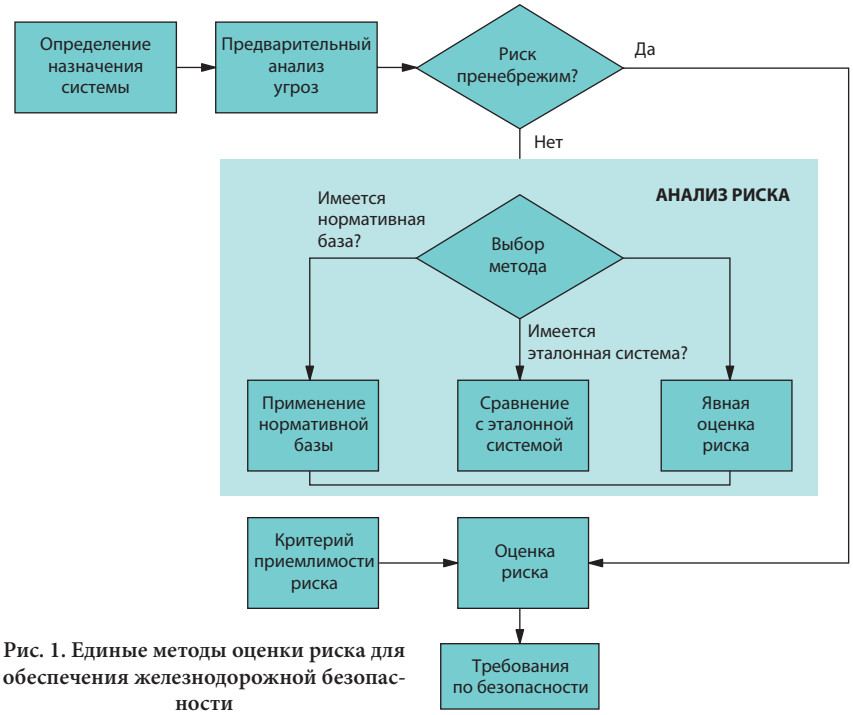

Рис. 1. Единые методы оценки риска для обеспечения железнодорожной безопасности

Детальное описание процесса обоснования требований по безопасности

Критерий приемлемости риска для технических систем

Эталонное значение критерия RAC-TS допустимости риска определено следующим образом: любой функциональный отказ, обладающий вероятным потенциалом непосредственного несчастного случая с катастрофическими последствиями, не должен происходить чаще, чем 10^{-9} за час эксплуатации.

Катастрофические последствия определены стандартом EN 50126–1 как «случаи гибели и (или) многочисленных увечий людей и (или) значительный ущерб окружающей среде».

Вероятный потенциал понимается в том смысле, что возникновение данного отказа должно сопровождаться вероятностью непосредственного несчастного случая с катастрофическими последствиями. Понятие «непосредственный» в данном контексте означает, что отсутствуют или почти отсутствуют какие-либо препятствия, способные предотвратить несчастный случай. Вероятный потенциал определяется по результатам расследования происшествий или несчастных случаев, на основе изучения соответствующих нормативных документов, на опыте предшествующей проектной деятельности, а также на основе консультаций со специалистами, обладающими опытом конкретной работы.

Единица измерения «операционный час» (unit) непосредственно

связана с функцией, в которой произошел отказ. Например, если такая функция локализуется на поезде, то операционным часом является один час его эксплуатационной работы. Такой подход означает, что, например, в системе уровня автоматической обеспечения безопасности движения поезда (automatic train protection — ATP), каждый вид отказа рассматривается отдельно.

Назначение критерия RAC-TS состоит в установлении единой метрики методов анализа риска, т. е. метрики, в которой могут быть, например, прокалиброваны матрицы риска.

Указанное выше значение критерия RAC-TS установлено как опорное значение допустимости риска, и риски с более высокой интенсивностью появления угроз или с более высокой значимостью их последствий считаются недопустимыми.

Для экстраполяции допустимости риска в область событий, не являющихся катастрофическими, в конкретных методах используются механизмы взвешивания рисков (этот процесс начинается обычно с использованием линейного взвешивания).

Предварительный анализ угроз

Наиболее ответственным решением является выбор уровня «незначительных» рисков, особенно когда это решение основывается на анализе, имеющем предварительный характер. Очевидно, что незначительный риск должен быть существенно ниже максимального риска, который еще остается допустимым для угроз данного класса. Поэтому предлагается считать угрозу незначительной, если связанный с нею риск по крайней мере на два порядка ниже максимально допустимого.

Очевидно также, что при этом необходимо определиться с точностью метода ранжирования риска; бессмысленно говорить о незначительном и максимальном допустимом риске, если погрешность их оценки составляет два порядка величины (рис. 2).

Рис. 2. Определение уровня незначительных угроз

Поэтому к методу ранжирования риска предъявляются следующие дополнительные требования:

- угрозы, критичность которых сопоставляется друг с другом, должны существовать на сопоставимых между собой уровнях идентификации систем;
- в качестве параметров угрозы должны быть приняты во внимание, по крайней мере, ее потенциальная значимость и потенциальная частота возникновения;
- для получения значимых и воспроизводимых оценок масштабирование параметров должно быть выражено количественно или описано настолько точно, насколько это позволит минимизировать ошибки принятия решений;
- параметры должны быть представлены в логарифмическом масштабе;
- незначительные изменения параметров угрозы не должны приводить к значительным изменениям ее критичности.
- если две угрозы обладают одной и той же критичностью, то и связанные с ними риски должны иметь величину одного и того же порядка.

Применение нормативной базы и оценка риска

Нормативная база безопасности представляет собой комплект правил в текстовой форме, корректное применение которых позволяет уменьшить опасность, представляемую угрозой. Нормативная база безопасности может быть международной или национальной, может существовать в виде стандартов, руководств и т. д. Нормативная база должна, как минимум, отражать текущий технологический уровень и передовой опыт деятельности на этом уровне в данной прикладной области; она должна быть применима к частным проблемам, доступна общественности и зарегистрирована соответствующими полномочными органами в области безопасности.

Если соответствие нормативной базе позволяет минимизировать угрозу согласно функциональным требованиям по безопасности, то применение этой нормативной базы закрывает опасность, связанную с угрозой, т. е. исключает необходимость в ее дальнейшем рассмотрении.

Применение сравнительного анализа для оценки риска

Цель сравнительного анализа — показать отсутствие ухудшения безопасности у новой системы по сравнению с эталонной, в качестве которой выступает уже существующая заменяемая или модернизируемая система. Здесь важно подчеркнуть, что при замене старых технологий или функций новыми необходимо сосредоточить анализ безопасности на их различиях, не допуская ухудшения безопасности при замене. Неизменяемые части или функции эталонной системы и среды ее функционирования при этом можно не рассматривать. При использовании такого подхода принципиально важным является предположение о том, что эталонная система в ее текущем функциональном контексте не является основным источником риска (это предположение справедливо для большинства технических систем), и о том, что она соответ-

ствует функциональным требованиям безопасности.

Сравнительный анализ сосредотачивается на различиях между новой и эталонной системами и на доказательстве того, что везде, где эти различия имеют место, предусмотрены меры, которые гарантируют сохранение существующего в эталонной системе уровня безопасности.

Эталонная система должна быть признана таковой, и на период проведения анализа это признание должно иметь силу. В идеале она должна обладать:

- тем же функциональным назначением;
- теми же функциями управления со стороны человека-оператора, особенно функциями человеко-машинного интерфейса;
- теми же возможностями по стойкости к воздействиям окружающей среды (обеспечиваемыми поставщиком);
- теми же интерфейсами;
- теми же угрозами, что эталонная система.

Обычно различия между новой и эталонной системами существуют. Сравнительный анализ все же может использоваться, если эти различия не ухудшают эффективность безопасности новой системы. Тем самым из сравнительного анализа могут быть получены прикладные требования по безопасности новой системы, т. е. требования по мерам безопасности, учитывающим специфику конкретного внедрения.

Если обеспечивается подобие новой и эталонной систем, то должны быть приняты во внимание следующие свойства эталонной системы:

- проектные требования в отношении полноты безопасности (случайной и систематической), эксплуатационная готовность (в тех случаях, когда она связана с безопасностью), удобство эксплуатации и руководства,
- требования по эксплуатации,
- требования по техническому обслуживанию.

В результате сравнительного анализа свойства эталонной системы могут быть транслированы в требования по безопасности новой системы и в доказательную базу неухудшения ее безопасности.

Применение метода явной оценки риска

Вообще говоря, качество процесса оценки риска при использовании этого метода контролируется и управляется на основе соответствия основным требованиям, приведенным в стандарте EN 50126-1 (особенно в части требований по компетентности, верификации и документации). При проведении явной оценки риска необходимо соблюдать следующие требования:

- результаты применения этого метода оценки риска должны иметь тот же формат (единицы измерения), что и требования по функциональной безопасности, т. е. если это требование выражается интенсивностью отказов (количеством отказов функции системы в течение часа ее эксплуатации), то результат оценки риска должен быть выражен в тех же единицах;
- должно быть представлено доказательство того, что при использовании принятого метода явной оценки риска не допускаются риски более высокие, чем установлено критерием RAC-TS;
- должно быть представлено доказательство того, что учтены все значимые параметры риска, связанного с эксплуатационным процессом, особенно время воздействия угрозы и возможность ее предотвращения или снижения последствий, задержка проявления неисправности после ее возникновения, время обнаружения отказа, являющегося результатом неисправности, время перехода в защитное состояние и серьезность неисправности;
- метод должен обеспечивать оптимизацию риска на множестве различных параметров, позволяя рассматривать комбинации вероятности опасного события и тяжести его последствий с целью применения критерия RAC-TS к угрозам, не являющимся катастрофическими;
- все параметрические выборки, промежуточные и окончательные результаты должны быть тщательно документированы, особенно в отношении единиц измерения и их соотношения;
- все используемые инструментальные средства должны быть поверены, либо должна быть обеспечена возможность проверки итоговых протоколов (например, вручную);
- точность количественных результатов должна находиться в пределах одного порядка измеряемой величины.

Требование по точности нуждается в небольшом пояснении. Точность задается размерами уровня полноты безопасности (safety integrity level, SIL), который, по определению, ограничивается величинами одного порядка. О такой точности свидетельствует также опыт IRSE ITC, в соответствии с которым погрешность анализа риска обычно локализуется в интервале одного или двух порядков величины.

Смысл этого требования состоит в том, что если тот же самый анализ выполняется дважды при тех же самых условиях (т. е. при тех же исходных данных, с тем же уровнем компетентности специалистов и т. д.), то при качественном выражении результата должен быть получен тот же уровень полноты безопасности (или почти тот же — для граничных случаев). Если требование выражено количественно, например, в виде допустимой интенсивности появления угроз (tolerable hazard rates, THRs), то для получаемых в результате анализа целевых значений интенсивности угроз HR_1 и HR_2 должно выполняться условие

$$|\log HR_1 - \log HR_2| \le 1. \qquad (1)$$

Требование по точности должно быть обеспечено на основе:

- анализа ошибок округления и ошибок экспертного обоснования (особенно в случае качественных или полуколичественных методов);
- оценки степени достоверности входных данных и результатов; при проведении вероятностной оценки риска (probabilistic risk assessment, PRA) величины HR_1 и HR_2 следует использовать в качестве верхней и нижней доверительных границ для целевого значения интенсивности угроз с учетом достаточно надежного попадания целевого значения в этот интервал (вероятность попадания не должна быть ниже 0,95).

Интеграция методов в комплексной модели риска

Предложения, содержащиеся в настоящей статье, отражают прежде всего потребности промышленности технических систем и средств железнодорожного транспорта в единых методах оценки риска CSM. Требуется подтвердить, что эти предложения вписываются в общую структуру единых целей в области безопасности CST и единых методов оценки риска CSM для железнодорожного транспорта, которые находятся вне сферы деятельности промышленности. Такое подтверждение действительно имело место — после расширенной экспертизы в специальной рабочей группе общий процесс в том виде, как он представлен на рис. 1, был утвержден ERA для комплексной оценки риска на железнодорожном транспорте.

Однако SAMNET отдает предпочтение количественной модели «галстук — бабочка» (bow-tie model), признавая при этом, что декомпозиция единых целей в области безопасности CST на технический уровень представляет значительную сложность (если вообще возможна). Тем не менее, несколько железных дорог в настоящее время пытаются разработать (частично) количественную модель оценки риска с целью определения того, обеспечивается ли в полном объеме достижение целей CST.

У такого подхода есть следующие недостатки и риски:

- по своему вкладу в безопасность движения эксплуатация и обслуживание имеют по меньшей мере такую же значимость, что и технические системы. Безопасность эксплуатации и обслуживания едва ли может измеряться только количественным выражением ошибок человека-оператора;
- железнодорожная система является сложной системой, в которой интегрированы различные технологии и которая функционирует в открытой среде (т. е. ее поведение и отказы не могут быть описаны полностью с применением только вероятностных методов);
- каждый национальный орган по безопасности имеет свой набор норм и правил. Расследование несчастных случаев и использование опыта являются основными элементами развития технологий обеспечения безопасности движения на железных дорогах.

Однако если используется вероятностная оценка риска PRA, то результаты подхода, предлагаемого UNIFE, могут быть интегрированы в комплексной модели риска следующим образом:

- если противодействие какой-либо угрозе регламентировано соответствующей нормативной базой, то можно исходить из настолько малой величины риска, связанного с этой угрозой, что она в количественной модели может быть приравнен к нулю;
- при использовании сравнительного анализа для оценки риска эффективность безопасности эталонной системы применительно к установленным для нее угрозам (определенная на основе аналитического либо статистического подходов) может быть непосредственно включена в модель «галстук — бабочка»;
- если была выполнена оценка риска, то полученное числовое значение может использоваться в качестве входа для количественной модели «галстук-бабочка».
- независимо от того, какой вход был использован, его следует рассматривать как постоянную величину, неизменяемую при проведении декомпозиции. В целом такой подход поддерживает незначительность вклада технических систем в обеспечение глобальных целей в области безопасности CST.

Интеграция этого подхода в глобальную модель риска, связанного с эксплуатацией железных дорог, имеет преимущества для всех заинтересованных сторон. Промышленность получает возможность работать со стандартными, гармонизированными требованиями по безопасности, а железнодорожным операторам нет необходимости предпринимать детальный анализ технических систем, которые сегодня вносят незначительный вклад в риск, связанный с работой железнодорожного транспорта.

J. Braband. Signal und Draht, 2007, № 4, S. 34–37.