МПЦ компании Bombardier для DBAG

Компания Bombardier выступает на международном рынке не только как изготовитель подвижного состава, но и в качестве поставщика устройств СЦБ и управления движением поездов. В настоящее время она разрабатывает систему микропроцессорной централизации (МПЦ) для железных дорог Германии (DBAG).

Разработкой МПЦ типа ESTW B950 для DBAG на основе технического задания ее дочернего предприятия DB Systemtechnik занимается компания Bombardier Transportation (Signal) Germany. Отраслевые отделы DB Systemtechnik осуществляют сопровождение процесса разработки и допуска к эксплуатации, который построен частично на основе документа Mü8004, но преимущественно на европейских стандартах EN50126, EN50128 и EN50129. Одновременно предусмотрено установить опытную систему МПЦ с напольным оборудованием на линии Мангейм — Райнау. В рамках пилотного проекта намечено также отработать технологию технического обслуживания новой техники. Сопровождая процесс разработки, представители DBAG особое внимание уделяют затратам жизненного цикла системы, включая повышение надежности и эксплуатационной готовности без ущерба для безопасной работы МПЦ.

МПЦ B950

Концепция МПЦ компании Bombardier основана на последовательном применении принципа децентрализации, реализуемого путем распределения интеллектуальных функций между всеми компонентами системы, что позволяет применять линии передачи данных для подключения различных устройств.

МПЦ содержит три уровня (рис. 1): управления (оперативного планирования), обеспечения безопасности (здесь реализуются маршрутные зависимости) и исполнительный (непосредственное управление напольными устройствами).

Уровень обеспечения безопасности

Компьютер централизации CS950 DB. Этот безопасно работающий компьютер рассчитан на обслуживание 150 – 200 напольных устройств. Применение шинной архитектуры позволяет соединять друг с другом до семи компьютеров CS950 DB. Из соображений эксплуатационной готовности компьютер выполнен в виде двух двухканальных систем, работающих каждая по схеме «2 из 2». В нормальном режиме одна система является рабочей, а другая находится в состоянии горячего резерва.

В вычислительных системах используется стандартизированная компьютерная платформа для ответственных приложений с операционной системой и базовым ПО, реализующим правила эксплуатации, заложенные в техническое задание. Особенности той или иной станции учитываются в проектных данных.

В ходе генерации исполняемого файла программы формируются контрольные суммы по отдельным библиотекам. Эти данные документируются и поставляются вместе с ПО. Имеется возможность в любое время считать контрольные суммы и номера версий того или иного файла. Благодаря этому при изменении проектных данных можно на основе контрольной суммы установить, используется ли в системе правильное ПО. Для этих целей органам приемки на DBAG предоставляется инструментарий, позволяющий в любое время проверить текущий статус программного обеспечения.

Сервисный модуль FEU образует сервисный интерфейс с компьютером централизации CS950 DB, через который осуществляется загрузка специализированного ПО для конкретной станции и файлов конфигурации. При помощи модуля FEU можно инициировать переключение с рабочего компьютера CS950 DB на резервный, а также получить диагностические данные, протоколы результатов работы системы, контрольные суммы и номера версий ПО.

Модуль EBISERV образует технологический интерфейс системы МПЦ с уровнем управления. Он отвечает за формирование защищенных от опасных искажений известительных данных. Кроме того, команды, введенные на уровне управления, подвергаются в этом модуле предварительной обработке и транслируются в компьютер централизации. EBISERV координирует исполнение команд, предусматривающих воздействие на несколько компьютеров централизации (например, команды на установку маршрута).

При выходе из строя соединения с рабочим местом дежурного по станции или регистрирующим компьютером данные, документирующие работу МПЦ, сохраняются в памяти EBISERV и передаются после восстановления соединения.

Через модуль EBISERV к аппаратуре уровня управления МПЦ может быть подключено до семи компьютеров CS950 DB.

Модуль EBISERV удовлетворяет требованиям обеспечения безопас-

ности уровня SIL4 согласно стандарту EN50129. Все выходные данные обоих безопасных вычислительных каналов сравниваются и выводятся только в случае совпадения. Модуль распознает в течение заданного времени единичные ошибки и переходит в защитное состояние. То же самое происходит, если превышается заданное время работы приложения. EBISERV основан на той же вычислительной платформе, что и компьютеры централизации, обеспечивая за счет резервирования высокую эксплуатационную готовность. Переключение с рабочего компьютера на резервный не ведет к приостановке технологического процесса.

Шина с высокоуровневым управлением потоками данных (HDLC). Обмен информацией между уровнем обеспечения безопасности (компьютерами CS950 DB) и исполнительным уровнем (модулями DCT) осуществляется по шине HDLC, имеющей кольцевую структуру и отвечающей стандарту EN50159 – 1.

Уровень управления

АРМ дежурного по станции. Уровень управления (рис. 2) включает в себя автоматизированное рабочее место дежурного по станции. Компьютер этого АРМ обеспечивает отображение на мониторах защищенных изображений и ввод ответственных команд. Дежурный по станции вводит команды при помощи мыши или клавиатуры. Схема путей может быть представлена в виде обзорного или детального изображения, другая информация, а также вводимые команды отображаются на контрольном дисплее. С его помощью дежурный по станции может обрабатывать данные планов автоматического управления установкой маршрутов. Информация, требующая протоколирования, выводится на регистрирующий принтер PSD и отображается на экране конт-

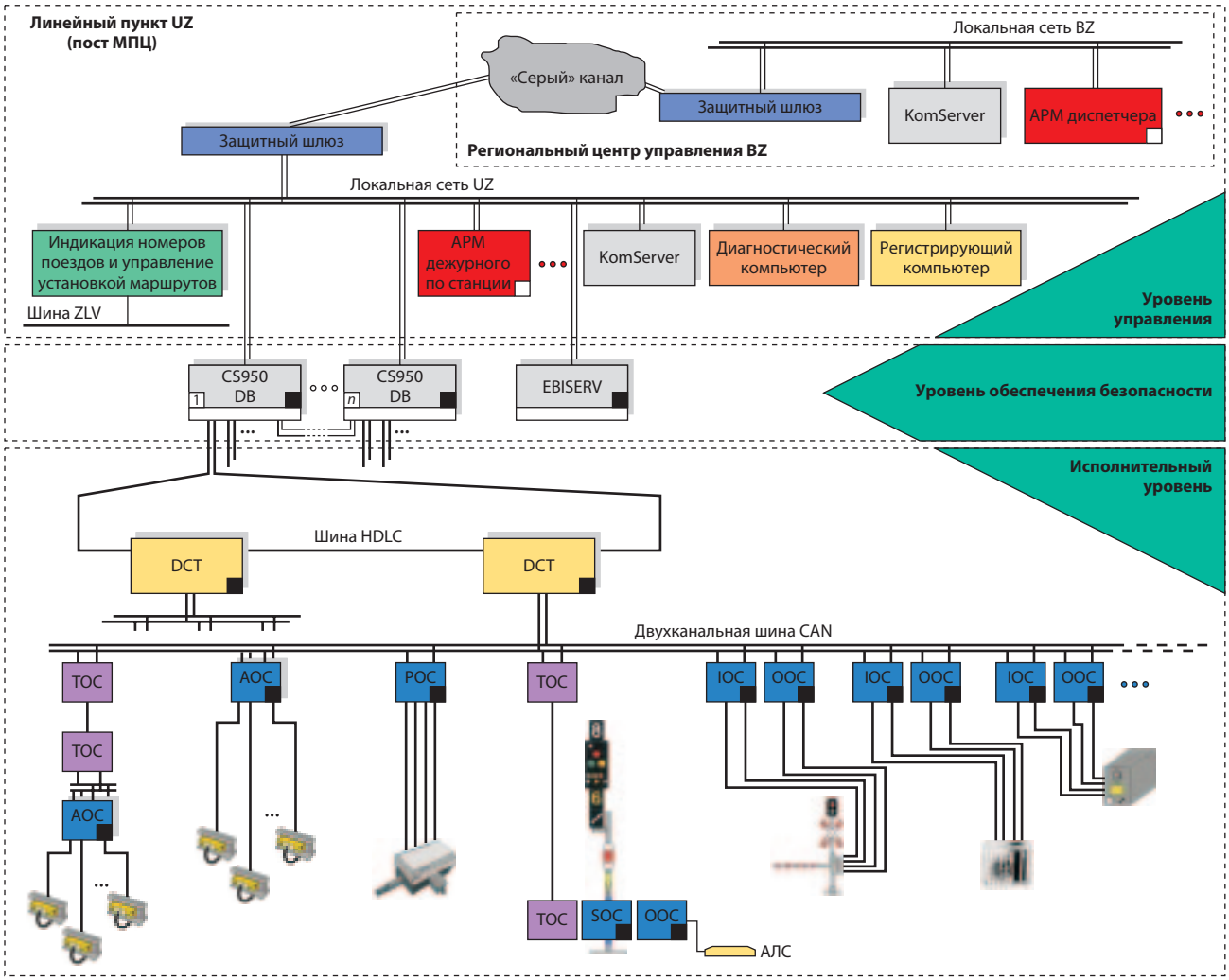

Рис. 1. Архитектура системы ESTW B950:
AOC — контроллер счетчиков осей; IOC — входной объектный контроллер; OOC — выходной объектный контроллер; POC — стрелочный контроллер; SOC — светофорный контроллер; TOC — объектный контроллер передачи данных; ZLV — слежение за движением поездов

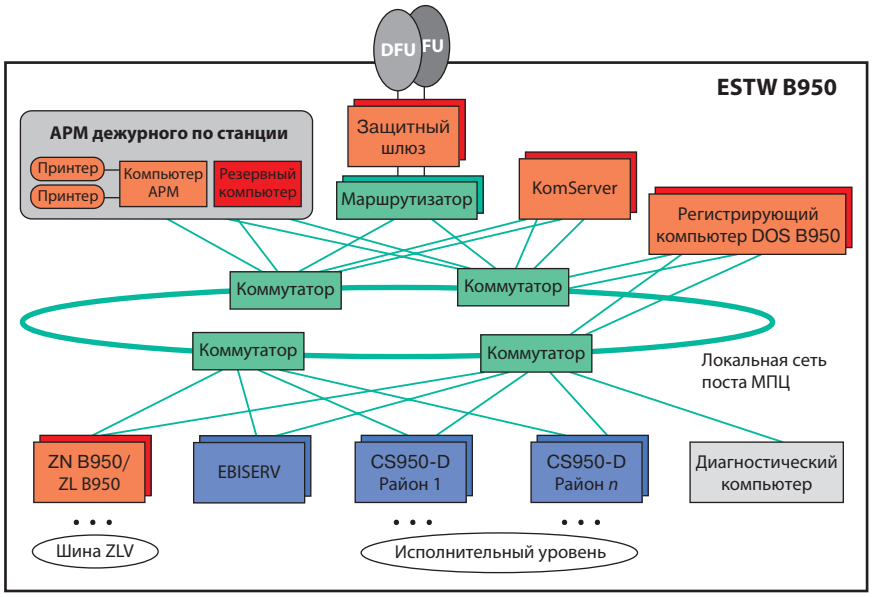

Рис. 2. Уровень управления МПЦ:
ZLV — слежение за движением поездов

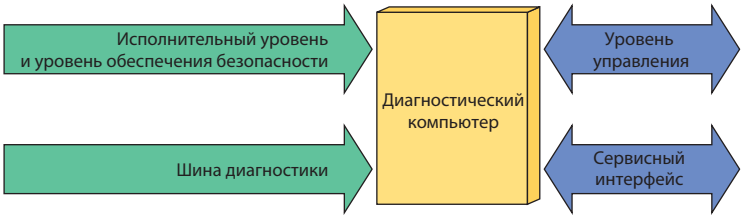

Рис. 3. Диагностический компьютер

рольного дисплея. АРМ построено на основе стандартного пользовательского интерфейса (SBS) и удовлетворяет требованиям работы поста МПЦ в режиме телеуправления. Благодаря этому систему ESTW B950 можно включать в зону действия регионального центра управления движением поездов DBAG.

Устройство индикации номеров поездов и компьютер автоматического управления установкой маршрутов. Для слежения за движением поездов, их идентификации и управления установкой поездных маршрутов на уровне управления используются устройство индикации номеров поездов (ZN) и компьютер управления установкой маршрутов (ZL). Устройство ZN определяет местоположение поездов и отображает их номера в соответствующих полях обзорного изображения схемы путей. Перемещение номера поезда из текущего поля в следующее осуществляется по закрытию напольного сигнала.

Информация о местоположении поездов берется из известительных данных МПЦ (при нахождении поезда на станции) или из шины слежения за поездами ZLV (если поезд находится на перегоне или соседней станции). Для автоматизации установки маршрутов предназначен компьютер ZL. В таблице использования путей (GBT) заложена возможность индикации и обработки суточных планов назначения маршрутов. Компьютер ZL извлекает информацию из этих планов и на ее основе автоматически управляет установкой маршрутов.

Все интерфейсы, кроме сопряжения с шиной ZLV, построены на основе протокола TCP/IP. Отдельные подсистемы взаимодействуют друг с другом не напрямую, а через коммуникационный сервер KomServer. Интерфейс с шиной ZLV реализован в устройстве ZN напрямую через модем. Устройства ZN и ZL могут работать на одной аппаратной платформе.

Ведение документации. Компьютер DOKU предназначен для ведения безбумажной документации на посту МПЦ. Он сохраняет протоколы, которые прежде распечатывались на принтере для регистрации технологического процесса и нарушений, а также на принтере устройства индикации номеров поездов, и обеспечивает ведение архива. Текущие сообщения передаются в компьютер АРМ дежурного по станции для отображения на экране монитора. При необходимости оператор может отобрать выдержки из массива извещений и распечатать их.

Диагностический компьютер (рис. 3) служит для анализа диагностических сообщений и извещений о ошибках МПЦ. Его задачами являются:

- сбор диагностических сообщений от всех подсистем МПЦ;
- сбор информационных и предупредительных извещений, а также извещений об нарушениях от всех подсистем МПЦ;
- непрерывное предоставление собранных извещений (при необходимости отфильтрованных) для отображения на экране монитора диагностического компьютера для ремонтного персонала DBAG, специалистов компании Bombardier и разработчиков, а также для дальнейшей трансляции через отдельный интерфейс с линией дальней передачи данных или локальной сетью (последняя функция реализована в виде дополнительной опции).

Физически диагностический компьютер подключен к локальной сети поста МПЦ и шине диагностики, взаимодействуя напрямую с подсистемой уровня управления МПЦ и компьютером

EBISERV, а также сервисным интерфейсом.

Локальная сеть поста МПЦ образует интерфейсы на уровне управления МПЦ и между этим уровнем и уровнем обеспечения безопасности. Сеть имеет кольцевую структуру и дублирована, поэтому ее единичный отказ не приводит к выходу из строя всей системы. Кроме того, соединения отдельных компонентов МПЦ с локальной сетью также дублированы. Сеть использует протокол TCP/IP и является закрытой согласно требованию стандарта EN50159 – 1.

Коммуникационный сервер KomServer, расположенный на уровне управления, служит для интерпретации информационных телеграмм SBS и их дальнейшей передачи. Для повышения эксплуатационной готовности коммуникационный сервер дублирован. KomServer может быть построен по каскадной схеме, что необходимо для подключения регионального центра управления к локальной сети поста МПЦ. Используя проектные данные, он распознает, какие информационные телеграммы предназначены для центра управления, и передает их в KomServer регионального центра, который отвечает за дальнейшее распределение этих данных.

Защитный шлюз (рис. 4) служит для обмена данными между линейным пунктом (постом МПЦ) и региональным центром управления через общедоступную сеть. Для предотвращения несанкционированного доступа к передаваемым данным защитный шлюз создает защищенное соединение, используя для этого так называемое тройное DES-шифрование с регулярной автоматической заменой ключа. Микросхема, реализующая шифрование, и запоминающее устройство размещены в блоке, защищенном от внешних воздействий. Каждое повреждение блока (механическое, химическое, электрическое или термическое) ведет к включению тревожной сигнализации и стиранию ключа и алгоритма шифрования.

Исполнительный уровень

Децентрализованный коммуникационный транскодер DCT предназначен для обеспечения связи между объектными контроллерами и компьютером централизации CS950 DB. Он осуществляет двустороннее преобразование протоколов между логическими или физическими объектными контроллерами (двухканальная шина CAN) и уровнем обеспечения безопасности (шина HDLC). В его задачи входит надежное (в том числе и в случае нарушений) предотвращение передачи извещений о неправильных состояниях в вышестоящую систему и несвоевременных выходных команд в объектные контроллеры. Транскодер построен по двухканальному принципу на платформе объектного контроллера. В нем предусмотрена проверка телеграмм в обоих каналах на идентичность. При частичных отказах аппаратных средств DCT переходит в безопасное защитное состояние. Высокая эксплуатационная готовность достигается за счет наличия резервного транскодера.

Шина CAN. Двухканальная шина CAN обеспечивает обмен командами и извещениями на исполнительном уровне. Обмен информацией осуществляется по принципу «главный — подчиненный», причем в роли главного (master) устройства всегда выступает транскодер DCT, а в роли подчи-

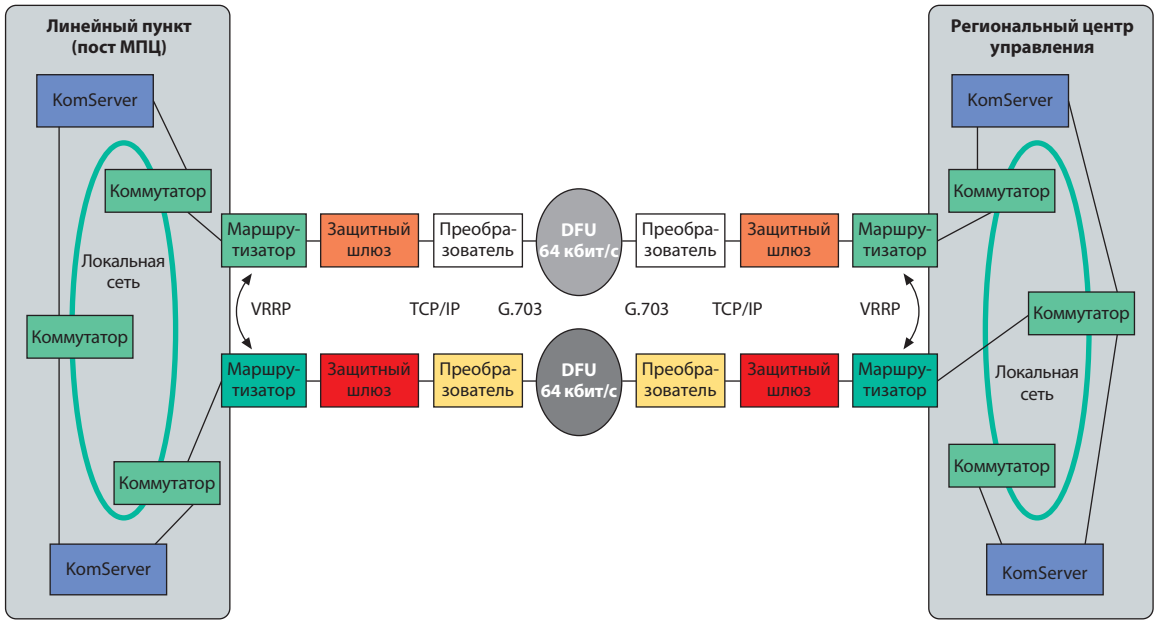

Рис. 4. Защитный шлюз:
KomServer — коммуникационный сервер; DFU — дальняя передача данных; VRRP, TCP/IP, G.703 — протоколы передачи данных

ненного (slave) — объектный контроллер. Для скорейшего извещения вышестоящей системы о состояниях напольных устройств обновление всех извещений осуществляется не реже чем каждые 300 мс. Благодаря этому извещения о состояниях и нарушениях поступают в систему в рамках заданного времени распознавания отказов.

Объектные контроллеры ОС основаны на универсальной аппаратной и программной платформе, расширяемой в зависимости от области применения при помощи соответствующих программных и аппаратных средств. Объектные контроллеры выполнены двухканальными, телеграммы в каналах сравниваются, и их несовпадение рассматривается как ошибка или нарушение. Блок питания оборудован устройством безопасного отключения. На дисплей устройства выводится информация о рабочих состояниях, нарушениях и т. п.

Коммуникационный контроллер ТОС делает возможным обмен информацией между объектными контроллерами, расположенными рядом с напольными устройствами, и постом централизации. При необходимости управления удаленными напольными устройствами за пределы поста МПЦ могут быть вынесены как отдельные контроллеры, так и их группы, объединенные в сеть. Передача данных основана на протоколе ISDN, что обеспечивает высокую гибкость в выборе среды (медный или волоконно-оптический кабель) и дальности передачи. При необходимости тракт передачи может дублироваться (две или четыре жилы в кабеле). Использование децентрализованных объектных контроллеров предполагает наличие ТОС по обе стороны тракта передачи. Соединение рассматривается как «серый» канал, при этом обмен телеграммами прозрачен и не предусматривает выполнения требований обеспечения безопасности.

Контроллер счета осей АОС применяется для надежного контроля за свободностью изолированных участков. Контроллер способен анализировать сигналы максимум от 32 пунктов счета осей и осуществлять контроль за ними. По результатам счета входящих и выходящих колесных пар проверяется свободность или занятость изолированных участков (путей и стрелок). Путевые датчики счетчиков осей и блоки подключения к ним поставляет компания Frauscher. Случайные ошибки в работе ведут к ограничению функциональности системы счета осей и не влияют на безопасность МПЦ. Извещение об ошибке влечет за собой сигнализацию занятия изолированного участка на уровне обеспечения безопасности, поэтому опасность ошибочного извещения о свободности стрелки или участка пути исключена. Для повышения эксплуатационной готовности контроллер АОС дублирован.

Стрелочный контроллер РОС. Этот объектный контроллер служит для управления стрелками и контроля за ними. Он способен независимо управлять двумя стрелками, подключенными по четырехпроводной схеме с рабочим напряжением 400 В. Несвоевременный перевод стрелки безопасно блокируется. Извещение о случайных ошибках ведет исключительно к ограничению функциональности, не влияя на безопасность системы в целом. Извещения о нарушениях передаются по шине CAN непосредственно на уровень обеспечения безопасности, поэтому возникновение опасной ситуации вследствие неправильного положения стрелки исключено.

Светофорный контроллер SOC обеспечивает безопасное управление сигналами и контроль за ними. К контроллеру может быть подключено до 10 светофорных ламп, при помощи которых можно вывести 32 сигнальных показания. В сочетании с контроллером ООС светофорный контроллер способен управлять другими устройствами, работающими на основе сигнальных показаний (например, точечной АЛС PZB, различными указателями и т. д.).

Контроллер безопасно блокирует несвоевременный вывод разрешающих показаний и передачу ошибочной информации о сигнальных показаниях в вышестоящую систему. В случае нарушений происходит немедленное контролируемое изменение сигнального показания на более запрещающее вплоть до закрытия сигнала или выключения его ламп.

Входной объектный контроллер IOC контролирует так называемые логические объекты, такие, как интерфейсы путевой блокировки и переездной сигнализации. Он способен считывать информацию максимум с 21 контакта и передавать ее в вышестоящую систему. Считывание информации о состоянии контактов происходит по двухканальной схеме через независимые цепи. О несовпадении данных в каналах сигнализируется в вышестоящую систему как о нарушении.

Выходной объектный контроллер ООС служит для управления логическими объектами посредством восьми беспотенциальных контактов, обеспечивающих безопасное сопряжение с интерфейсами систем блокировки или переездной сигнализации, а также контроль за ними. Предусмотрено последовательное включение контактов двух реле, каждое из которых подключено к своему вычислительному каналу. Контроллер способен командами проверять положение контактов и при его несовпадении с заданным переходить в защитное состояние, останавливая свою работу.

Устройство электроснабжения STV выдает для всех систем одно напряжение — 400 В. Из этой сети каждая подсистема генерирует требуемое напряжение питания. Для повышения эксплуатационной го-

товности дополнительно предусмотрен источник бесперебойного питания, подключенный к агрегату резервного питания. Он способен обеспечивать электроснабжение МПЦ в течение от 1 до 3 ч.

Документация

Допуск к эксплуатации по нормам CENELEC требует сквозного ведения документации в течение всего жизненного цикла системы. На каждом этапе реализации проекта документировались все результаты работы, т. е. для каждого этапа можно проследить все действия в сферах управления проектом, разработки, верификации, валидации, управления качеством и т. д. В отдельном перечне приведены все создаваемые в рамках проекта документы. Федеральное бюро железнодорожного транспорта EBA устанавливает перечень документов, требующих экспертизы, с указанием, какая инстанция будет эту экспертизу проводить.

Верификация и валидация

Верификация и валидация должны подтвердить, что система в полной мере отвечает всем предъявляемым требованиям. Действующие требования, являющиеся основой для валидации базовой системы микропроцессорной централизации компании Bombardier, содержатся в следующих документах:

- стандартах EN50126, EN 50128, EN50129, IEEE Std 1012 – 1986 и др.;
- спецификациях (системной, тестирования системы, анализа опасных ситуаций, описании архитектуры);
- планах (безопасности, обеспечения качества, концепции тестирования, ведения документации, управления конфигурацией);
- причастных документах (техническом задании DBAG на системы МПЦ, анализе рисков МПЦ).

Действия, связанные с верификацией, согласованы с валидацией и установлены в перечнях проверочных мероприятий. Эксперты по валидации контролируют эти действия на всех этапах разработки системы.

Рабочая группа экспертов по валидации должна получить практическое подтверждение того, что выполнены все требования к устройствам СЦБ, содержащиеся в технических заданиях DBAG, системных спецификациях и анализе опасных ситуаций. Порядок действий при верификации и валидации изложен в стандартах EN 50128 и EN50129.

Кроме того, в ходе валидации необходима полная проверка подсистем CS950 DB, включая их внешние интерфейсы. Все тесты должны допускать повторное воспроизведение и протоколироваться в форме, допускающей последующий аудит. По стандартам CENELEC программное обеспечение, рассчитанное на выполнение ответственных функций, должно соответствовать уровню безопасности SIL4. После завершения всех этапов верификации составляется окончательный отчет.

Состояние пилотного проекта

В настоящее время система микропроцессорной централизации компании Bombardier проходит процедуру допуска к эксплуатации со стороны EBA. В МПЦ использованы объектные контроллеры, которые уже имеют допуск по документу Mü8004 (рис. 5). Другие разрабатываемые подсистемы проходят процедуру допуска по нормам CENELEC, а также правилам строительства и эксплуатации железных дорог Германии и другим действующим в стране инструкциям и правилам, касающимся железнодорожного транспорта.

Рис. 5. Аппаратура МПЦ ESTW B950

Проект для линии Мангейм — Райнау

Пилотный проект МПЦ компании Bombardier реализуется на линии Мангейм — Райнау железных дорог Германии и предусматривает замену двух постов механической централизации и одного релейной типа SpDrS59. Система МПЦ ESTW B950 на станции Райнау и в пункте ответвления Неккарау контролирует двухпутный электрифицированный участок длиной 10 км. В Неккарау от участка ответвляется однопутная электрифицированная линия к сортировочной станции Мангейм. Максимально допустимая скорость движения поездов составляет 160 км/ч.

В Райнау расположен распорядительный пост МПЦ, в Неккарау и на соседних станциях — децентрализованные исполнительные посты.

В зону действия системы ESTW B950 входят 60 светофоров, 31 электроприводная стрелка, 84 пункта счета осей, 58 систем счета осей, пять электрических устройств запирания путей, одна установка переездной сигнализации и пять интерфейсов с устройствами путевой блокировки типа Sb 59.

R. Sölch, M. Burkhard. Signal und Draht, 2005, S. 25 – 30.