СИСТЕМЫ АВТОМАТИЗАЦИИ В НАУЧНЫХ ИССЛЕДОВАНИЯХ И ПРОМЫШЛЕННОСТИ

УДК 004.5 + 004.75

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ ОБЪЕКТАМИ ПОВЫШЕННОЙ ОПАСНОСТИ

С. А. Белоконь, В. В. Васильев, Ю. Н. Золотухин, А. С. Мальцев, М. А. Соболев, М. Н. Филиппов, А. П. Ян

Учреждение Российской академии наук
Институт автоматики и электрометрии Сибирского отделения РАН,
630090, г. Новосибирск, просп. Академика Коптюга, 1
E-mail: michael@idisys.iae.nsk.su

Предложен метод построения систем диспетчерского управления объектами повышенной опасности, представлены архитектура аппаратного комплекса и принципы организации программного обеспечения, а также разработанная на их основе автоматизированная система управления движением поездов Новосибирского метрополитена.

Ключевые слова: автоматизированная система диспетчерского управления, объекты повышенной опасности, SCADA-система, управление движением поездов метрополитена.

Введение. Среди широкого спектра систем автоматизированного управления особое место занимают системы диспетчерского управления (АСДУ), предназначенные для использования на объектах повышенной опасности, таких как предприятия атомной и химической промышленности, транспортные комплексы, объекты военного назначения и т. д., нарушения в работе которых представляют прямую угрозу жизни и здоровью людей.

Начиная с 2004 г. Институт автоматики и электрометрии СО РАН с участием ведущих специалистов службы сигнализации и связи Новосибирского метрополитена разрабатывает автоматизированную систему диспетчерского управления движением поездов; с 2005 г. система поэтапно вводится в постоянную эксплуатацию [1].

Используемая в метрополитене АСДУ обязана удовлетворять более высоким, чем типовые, требованиям по надёжности и безопасности, поскольку от её работоспособности непосредственно зависит безопасность пассажиров.

Серьёзным требованием при выборе средств автоматизации является режим функционирования транспортного комплекса, ограничивающий непрерывное время работы по модернизации и последующему тестированию АСДУ несколькими ночными часами, что практически исключает возможность единовременного обновления всех компонентов. Поэтому система должна обеспечивать постепенную интеграцию с существующей разнородной аппаратно-программной средой и поэтапное переключение функций с поддержкой режима одновременной работы заменяемой и новой частей в течение опытной эксплуатации.

Эти условия могут быть выполнены с минимальными издержками лишь в том случае, если АСДУ является модульным, легко расширяемым и динамически конфигурируемым комплексом, разработанным в соответствии со стандартами открытых систем, т. е. согласно определению международного стандарта IEEE POSIX 1003.0 реализует открытые спецификации интерфейсов, служб и форматов данных, достаточные для того, чтобы обеспечить: возможность переноса прикладных систем, разработанных должным образом,

с минимальными изменениями на широкий диапазон систем; совместную работу с другими прикладными системами на локальных и удалённых платформах; взаимодействие с пользователями в стиле, облегчающем последним переход от системы к системе [2].

1. Постановка задачи. При разработке как аппаратных средств, так и программного обеспечения (ПО) систем управления объектами повышенной опасности недостаточно лишь организации дополнительного резервирования составляющих, поскольку помимо высокой надёжности при работе в штатном режиме весь программно-аппаратный комплекс должен обеспечивать предсказуемо-безопасное поведение в случае выхода из строя отдельных компонентов.

Ограничения, налагаемые конкретными объектами управления, а также перечень требований, регламентируемых государственными, отраслевыми и внутренними стандартами предприятий, не позволяют найти полностью готовое универсальное решение, но тем не менее дают возможность предложить базовую архитектуру аппаратного комплекса и принципы организации ПО, достаточные для построения надёжных и безопасных систем диспетчерского управления объектами повышенной опасности.

Необходимость в математическом обеспечении, учитывающем варианты развития событий, вызвана также и отличием АСДУ от полностью автоматических систем: диспетчерское управление предполагает первостепенное и активное участие человека, поэтому анализ отдаваемых им команд и блокирование ошибочных действий в режиме реального времени является необходимым условием гарантии безопасности, позволяющим уменьшить влияние так называемого «человеческого фактора».

Ещё на этапе проектирования подобное усложнение логики работы может значительно затруднить оценку характеристик создаваемой системы, основными из которых являются надёжность, безопасность и живучесть [3]. И если для аппаратной части, составленной из стандартных компонентов, можно воспользоваться предоставляемыми производителями данными о среднем времени наработки на отказ, сроке службы и т. п., то для программной статистический подход, по крайней мере на первом этапе, неприменим ввиду уникальности системы управления и планируемого штучного использования. Таким образом, существует необходимость разработки принципов организации ПО, позволяющих составлять сложные и логически непротиворечивые программные комплексы из поддающихся анализу относительно простых модулей.

На основе изложенного можно сделать вывод, что основными задачами при разработке систем управления объектами повышенной опасности являются:

— обеспечение повышенной надёжности программно-аппаратного комплекса и безопасного поведения при отказах;

— ограничение несанкционированного доступа к управлению и данным системы;

— снижение негативного влияния человеческого фактора.

2. Предложенное решение. 2.1. *Структура и функции системы.* Разработанная АСДУ движением поездов представляет собой трёхуровневую структуру, состоящую из комплекса автоматизированных рабочих мест (АРМ) и программируемых логических контроллеров (ПЛК), распределённых на значительном пространстве и функционирующих в темпе реального технологического процесса [4]. Система объединяет распределённую микропроцессорную систему и маршрутно-релейные централизации (МРЦ) на каждой станции (рис. 1).

Верхний уровень системы включает в себя оборудование, установленное на центральном посту управления: основной и резервный АРМ поездного диспетчера, АРМ дежурного инженера диспетчерской централизации и сервер базы данных.

Средний уровень — расположенные на станциях рабочие места дежурных по станции и электромехаников.

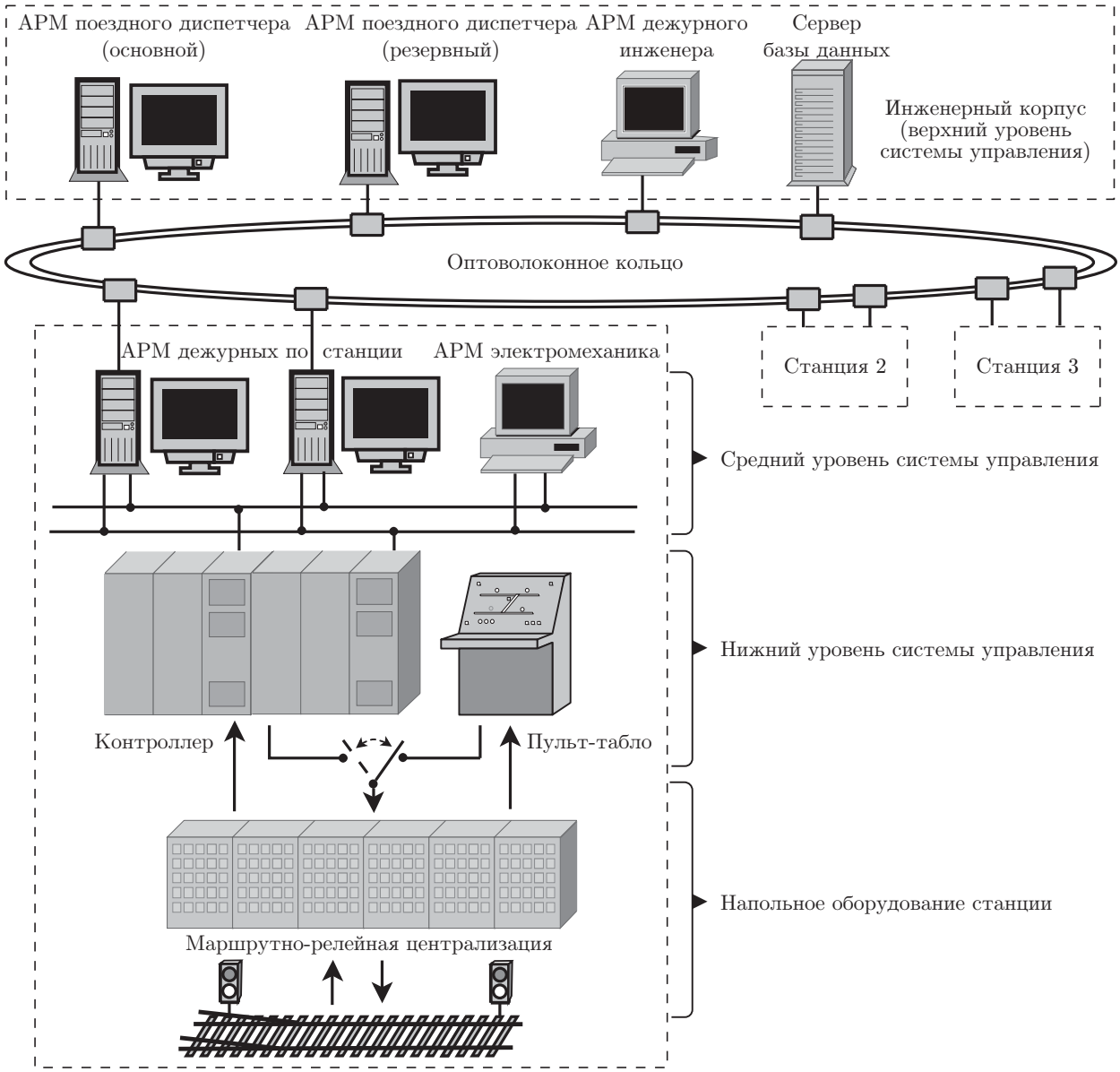

Рис. 1. Архитектура АСДУ движением поездов

Нижний уровень — программируемый логический контроллер, выполняющий функции устройства сопряжения с объектом и реализующий алгоритмы управления напольным оборудованием.

Аппаратура верхнего и среднего уровней объединена двойным оптоволоконным кольцом, обеспечивающим необходимую скорость и надёжность доставки данных. Автоматизированные рабочие места на каждой станции связаны с программируемым логическим контроллером и между собой посредством локальной станционной сети с резервированием. Для обеспечения непрерывного управления движением на время сервисного обслуживания или в случае выхода из строя микропроцессорной части системы предусмотрено быстрое переключение на традиционную схему с использованием пульта-табло, полностью отключающее ПЛК от каналов управления.

Управление движением поездов осуществляется либо с АРМ поездного диспетчера центрального поста, либо с расположенных на станциях АРМ дежурных, при этом АСДУ

обеспечивает выполнение следующих основных функций [5]:

— обработка информации и представление оператору состояния технологических объектов на станциях линии метрополитена в режиме реального времени;

— предоставление оператору средств управления технологическими объектами (задание маршрутов приёма и отправления, режимов автодействия, перевод стрелок, открытие пригласительных сигналов и т. д.);

— контроль правильности действий оператора и поддержка системы статических и динамических подсказок, проверка возможности исполнения введённых команд (свободность стрелочной секции и незамкнутость стрелки в маршруте при попытке перевода стрелок, отсутствие установленных враждебных маршрутов, незанятость путевых и стрелочных секций при задании маршрута и т. п.);

— многоуровневое динамическое разграничение доступа к управлению различных групп операторов с привязкой к контролируемым системам;

— протоколирование действий оперативного персонала, внешних событий и функционирования аппаратуры МРЦ;

— просмотр в динамическом режиме состояния устройств автоматики и поездной ситуации на станции за любой период времени, включая режим реального времени;

— доступ к технологической информации с любого АРМ электромеханика в пределах системы.

2.2. *Особенности архитектуры.* Одним из отличий предложенной архитектуры АСДУ от классической схемы с иерархией «основной—резервный» является параллельная рассылка копий команд управления по нескольким независимым каналам (рис. 2).

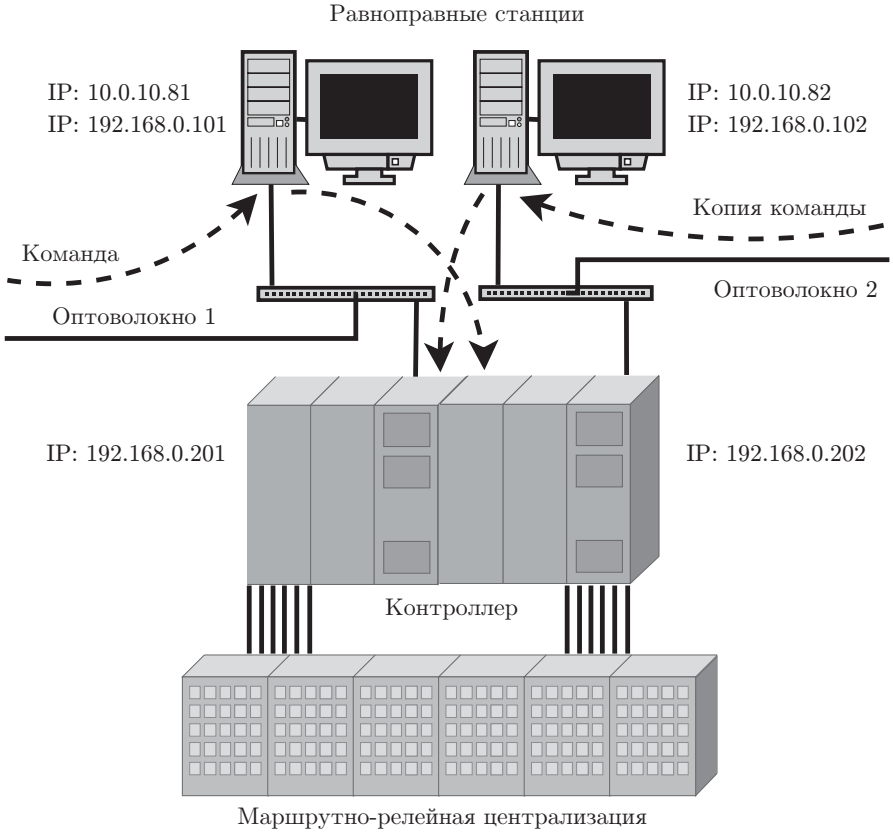

Рис. 2. Архитектура АСДУ на основе равноправных серверов

В рамках этой модели принимаемые команды анализируются асинхронно работающими равноправными серверами перед отправкой на нижележащий уровень (контроллер); последний, в свою очередь, выполняет первую полученную команду и запоминает её уникальный идентификатор вместе с результатом исполнения, которые затем используются при формировании ответов на поступающие позже копии.

Таким образом, при выходе из строя одного из каналов доставки и обработки команд, включая компьютеры, маршрутизаторы, оптоволоконный кабель, сетевой модуль ПЛК и др., выполнение задания и получение ответа на отправленный запрос происходит по дополнительной линии связи. При этом отсутствуют обычные (и зачастую существенные — до нескольких секунд) задержки перед переключением на резервное оборудование и повторную посылку сообщения, что обеспечивает не только повышенную отказоустойчивость системы, но и быстродействие, необходимое при выполнении экстренных команд оператора.

На момент получения команды внутреннее состояние модулей логики серверов в общем случае различно, поскольку, работая в асинхронном режиме, они опрашивают контроллер в различные моменты времени. Как показано в [6], посвящённой оценке надёжности ПО, это значительно уменьшает вероятность одновременного отказа обоих узлов в случае ошибок, проявляющихся при определённых состояниях входов системы.

Аппаратно первое и второе АРМ дежурных по станции подключены к сетевым маршрутизаторам, находящимся в противоположных фойе станции метрополитена на значительном расстоянии друг от друга, причём каждый из маршрутизаторов соединён с обоими каналами оптоволоконного кольца, обеспечивая надёжную передачу данных и функционирование всей системы в случае отключения энергоснабжения, пожара или затопления в одном из серверных помещений, что повышает общий уровень катастрофоустойчивости.

Помимо исполнения основной задачи системы (надёжной и своевременной передачи информации о поездной ситуации со станции на рабочие места дежурных и команд управления в обратном направлении) отдаваемые оператором команды должны анализироваться ПО в целях выявления несогласованных и потенциально опасных действий, способных привести к нештатной или аварийной ситуации.

Для соблюдения данного требования каждое действие оператора анализируется независимо друг от друга тремя различными подсистемами: ПО АРМ поездного диспетчера, АРМ дежурного по станции, в распоряжении которого находятся полные сведения о состоянии контролируемого участка линии, и, наконец, контроллером — согласно ограниченному (в целях снижения объёма вычислений и повышения быстродействия) набору наиболее актуальных проверок, осуществляя тем самым оперативную реакцию на изменение поездной ситуации.

Таким образом, многоуровневый анализ действий диспетчера производится несколькими подсистемами, реализованными независимыми разработчиками с использованием различных языков программирования, что предоставляет необходимый уровень диверсификации.

Существенным достоинством предложенной архитектуры является обеспечение многоуровневого анализа безопасности действий оператора, повышенной живучести системы и восстановления рабочего состояния в случае выхода из строя её составляющих. Дополнительное преимущество схемы с равноправными серверами состоит в возможности изменения конфигурации без перезапуска остальной части системы, например, для подключения дополнительных резервирующих узлов и линий связи, выключения части оборудования на профилактическое обслуживание, а также поэтапной замены программного и аппаратного обеспечения с предварительным тестированием в параллельном режиме.

2.3. *Особенности программного обеспечения.* В настоящее время подавляющее большинство SCADA-систем предназначено для использования исключительно в операционной

системе Windows, а буквально единицы оставшихся либо не составляют им конкуренции в плане функциональности, либо разработаны для какой-то конкретной операционной системы и не являются многоплатформенными. Это — серьёзное препятствие при разработке распределённых систем, в которых к отдельным узлам предъявляются повышенные требования по отказоустойчивости (что требует использования хорошо зарекомендовавших себя решений на базе операционных систем QNX или GNU/Linux), а второстепенные узлы, реализующие только функции наблюдения, могут представлять собой стандартные персональные компьютеры с более привычной для пользователей и обслуживающего персонала операционной системой MS Windows.

Исследования надёжности систем АСУ ТП показывают, что значительное количество критических ошибок, существенно снижающих уровень информационной безопасности управляющих комплексов, ежегодно выявляется как в операционной системе MS Windows, так и в коммерческих SCADA-системах [7].

Таким образом, не менее важным фактором при выборе ПО является возможность доступа к исходным текстам в целях непредвзятого анализа надёжности, исследования недокументированных особенностей поведения и при необходимости независимого от разработчика и оперативного расширения функциональности.

Приведённые выше требования положены в основу спецификаций открытой многоплатформенной SCADA-системы. При её разработке активно применялся принцип модульности (построение из автономных элементов с простыми и согласованными структурными связями между ними) для обеспечения гибкости и расширяемости архитектуры, упрощения повторного использования кода, а также повышения надёжности программы.

Предсказуемо безопасное поведение в условиях неполной или недостоверной информации достигается путём обработки данных на основе варианта трёхзначной логики [8], представляющего собой расширение классической бинарной логики дополнительным истинностным значением, которое интерпретируется как отсутствие в данный момент информации о точном значении переменной или нарушение одного из заданных ограничений во время вычисления выражения. Преимуществом предложенного метода является то, что он позволяет наряду с точными данными оперировать неполной информацией, унифицируя и существенно упрощая при этом запись логических выражений.

Внутренняя архитектура SCADA-системы подчинена разработанной концепции динамического программного интерфейса. Основной его идеей является организация всех разделяемых между частями системы точек взаимодействия в виде единой динамически изменяющейся структуры. С точки зрения модуля регистрация (или публикация) собственного интерфейса выглядит как операция создания нескольких элементов в специализированной виртуальной файловой системе, поддерживающей функции работы с объектами, организованными в виде древовидной структуры с узлами-каталогами, а в качестве имени-идентификатора выступает строка с символом-разделителем между элементами — путь от корневого каталога до конкретного объекта [9].

В качестве иллюстрации на рис. 3 приведена типовая конфигурация ПО АРМ дежурного по станции, состоящая из шести одновременно работающих модулей, которые взаимодействуют по протоколу TCP/IP: модуль маршрутизатора (hub) предназначен для пересылки сообщений между компонентами системы; модуль пользовательского интерфейса (viewer) обеспечивает отображение графической информации на экране оператора и передачу вводимых команд модулю логики (logic) для дальнейшей обработки; модуль связи (modbus) передаёт проверенные модулем логики команды в контроллер, а также периодически опрашивает состояние переменных контроллера и генерирует сообщения об изменениях; модуль базы данных (shn_writer) заносит в неё записи об изменении состояния системы; наконец, модуль dch_server обеспечивает связь с верхним уровнем АСДУ. Пример пользовательского интерфейса оперативного персонала приведён на рис. 4.

Рис. 3. Схема взаимодействия модулей ПО АРМ дежурного по станции

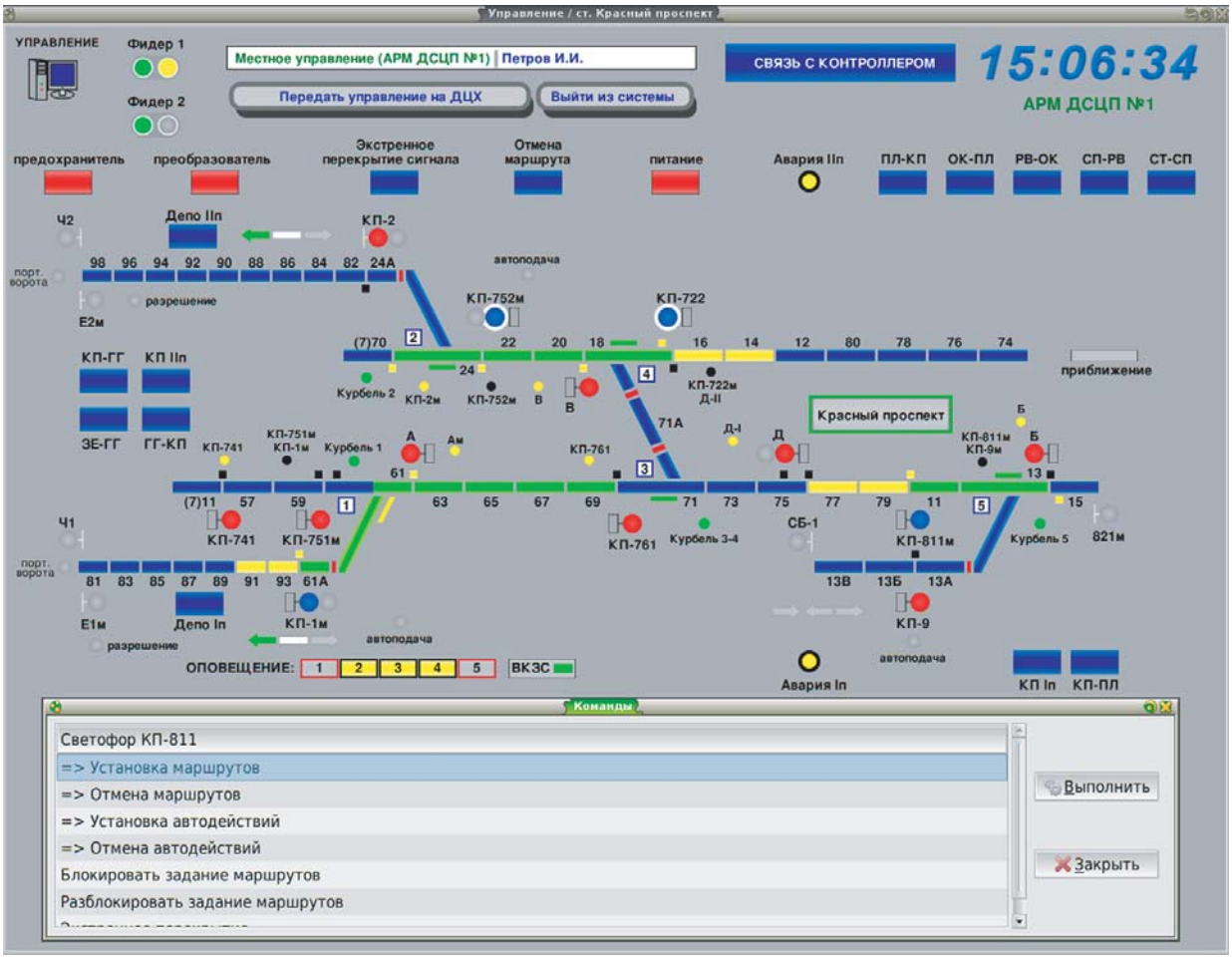

Рис. 4. Видеокадр АРМ дежурного по станции «Красный проспект»

Существенное сокращение времени разработки приложений достигнуто за счёт поддержки открытых стандартов. Например, поскольку все конфигурационные файлы системы, включая описания отображаемых на экране объектов, основаны на формате XML, разработчику предоставляется возможность выбора не только наиболее удобного в каждом конкретном случае приложения-редактора, но и системы управления версиями для работы со всеми файлами программного продукта, в том числе графической информацией.

Интегрированная поддержка сценариев позволяет реализовать концепцию выработки для конкретной задачи предметно-ориентированного языка (DSL — Domain-Specific Language), значительно сократить объём работы программиста, а также повысить надёжность ПО благодаря корректной обработке интерпретатором типичных ошибок исполнения.

Предложенная архитектура даёт возможность разрабатывать программные комплексы со сложными логическими зависимостями между частями, составляя динамическую конфигурацию из подгружаемых модулей.

Для оценки надёжности ПО использован метод, позволяющий учесть особенности индивидуальной истории создания программы, заключающийся в выявлении зависимости количества значимых изменений кода от фактического времени разработки по предоставляемой журналом системы управления версиями информации и экстраполяции полученной функции в целях получения числовых оценок остаточного количества ошибок и скорости их обнаружения [10].

На базе данной SCADA-системы создано ПО АРМ дежурного по станции, АРМ электромеханика, АРМ инженера центрального поста, разработаны средства для анализа в пошаговом режиме архивных данных. В качестве иллюстрации на рис. 5 приведён пример пользовательского интерфейса эксплуатационного персонала.

На основе операционной системы GNU/Linux создана универсальная конфигурация ПО АРМ, которая не содержит коммерческих программ или компонентов с закрытым исходным кодом. Система настроена на автоматический запуск единственного приложения с правами пользователя, не допускающими модификации программного обеспечения и архивных данных.

2.4. *Моделирующий стенд.* По существующему регламенту перед вводом системы в опытную эксплуатацию должна быть проведена комплексная отладка технических и программных средств в лабораторных условиях. Для этого в рамках работы по созданию автоматизированной системы диспетчерского управления движением поездов Новосибирского метрополитена создан моделирующий стенд [11]. В состав стенда входит программно-аппаратный комплекс, осуществляющий моделирование аппаратуры маршрутно-релейной централизации и напольного оборудования станции, программируемый контроллер, а также автоматизированные рабочие места оперативного и эксплуатационного персонала (рис. 6).

Аппаратная часть данного комплекса представляет собой систему, включающую компьютер, моделирующий напольное оборудование, программируемый логический контроллер, имитирующий МРЦ, и коммуникационные подсистемы.

Программное обеспечение моделирующего комплекса разработано на основе описанной выше SCADA-системы и реализует необходимые для тестирования АСДУ ситуации, такие как движение поездов, включение/выключение светофоров, перевод стрелок, неисправности оборудования (перегорание лампы светофора, потеря контроля стрелки, ложная занятость рельсовой цепи и т. п.).

Моделирующий комплекс позволяет тестировать программное и аппаратное обеспечение разрабатываемой АСДУ до начала монтажа оборудования на станции, а также при необходимости воспроизвести и проанализировать ситуации, происходившие на реальных

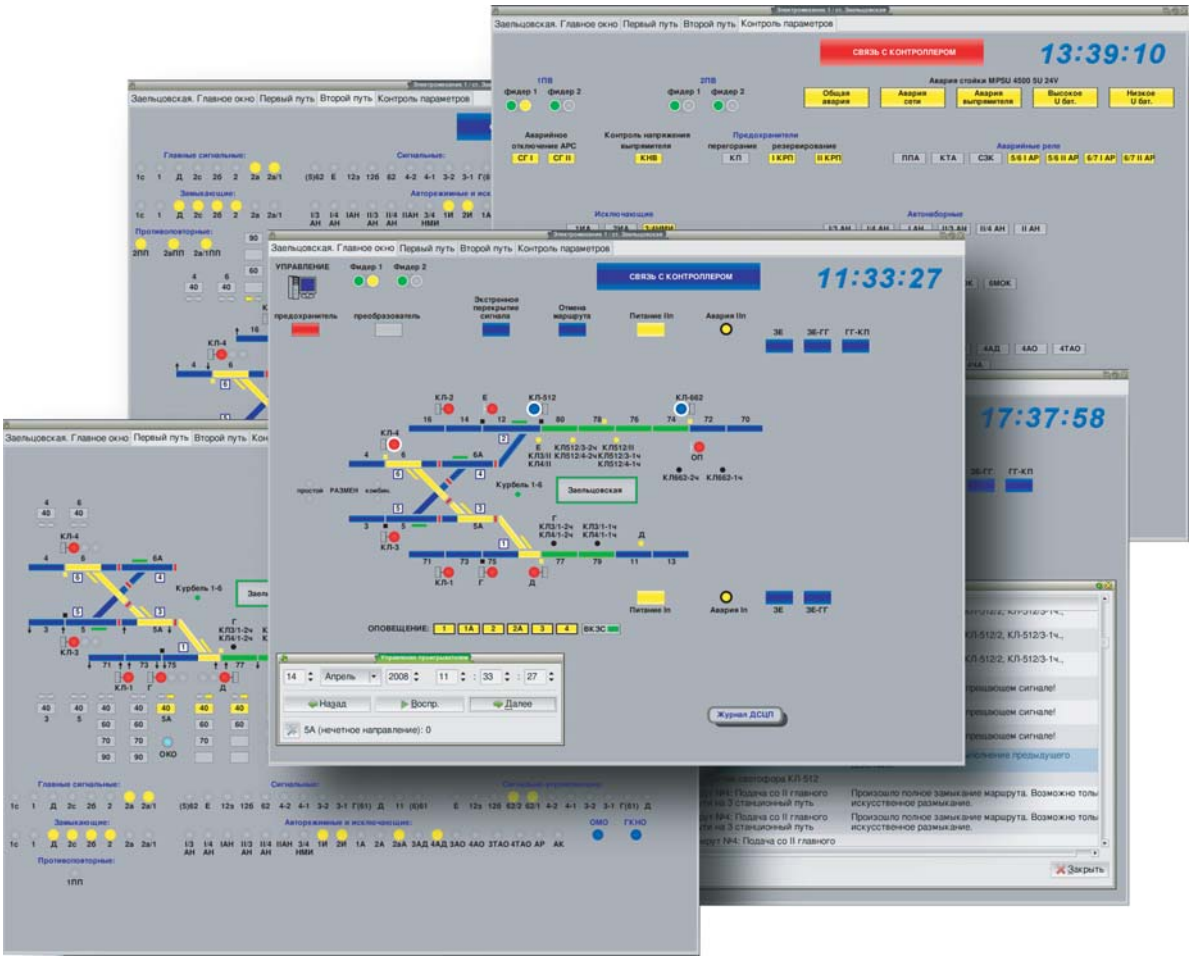

Рис. 5. Видеокадры АРМ электромеханика станции «Заельцовская»

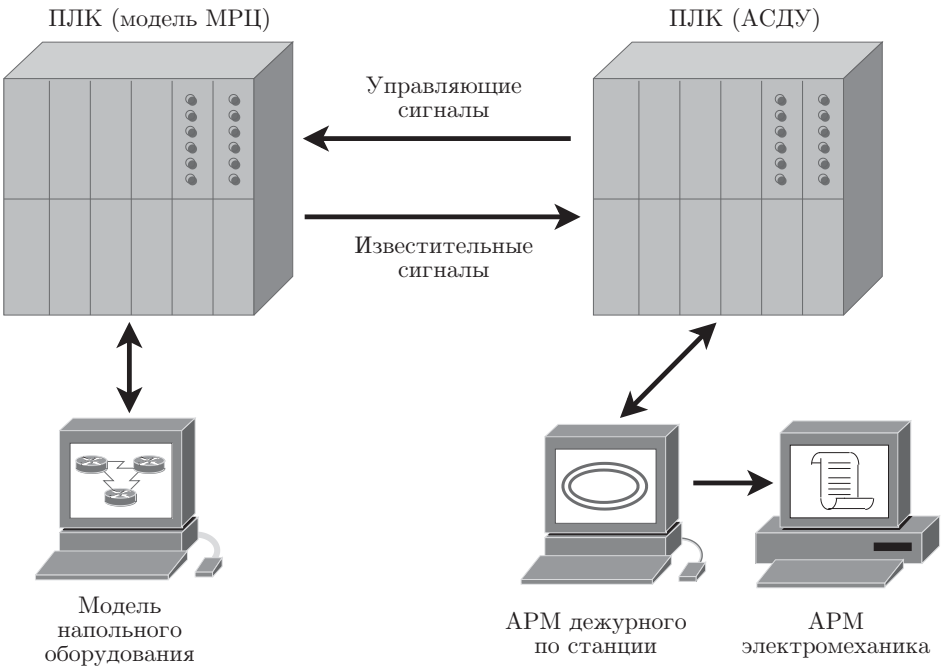

Рис. 6. Схема моделирующего стенда

Рис. 7. Видеокадры измерительной подсистемы станции «Берёзовая роща»

станциях метрополитена, что дополнительно даёт возможность использовать его в качестве тренажёра для оперативного и эксплуатационного персонала.

2.5. *Измерительная подсистема.* Для решения задачи мониторинга состояния оборудования разработана подсистема [12], которая обеспечивает измерение аналоговых сигналов и анализ накопленных данных в целях выявления трендов параметров аппаратуры, а также оценку остаточного ресурса устройств, таких как стрелочные электроприводы, реле, светофорные лампы и др.

На рис. 7 приведены примеры пользовательского интерфейса измерительной подсистемы.

Заключение. В представленной работе предложен подход к построению автоматизированных систем диспетчерского управления объектами повышенной опасности, на основе которого создана автоматизированная система диспетчерского управления движением поездов Новосибирского метрополитена. Система обеспечивает повышение эффективности работы оперативного и эксплуатационного персонала, протоколирование действий дежурных и непрерывную регистрацию работы устройств маршрутно-релейной централизации.

К настоящему моменту система введена в постоянную эксплуатацию на станциях «Берёзовая роща», «Площадь Гарина-Михайловского», «Заельцовская», «Красный проспект», «Сибирская» и «Золотая нива».

СПИСОК ЛИТЕРАТУРЫ

1. **Абрамов А. И., Белоконь С. А., Васильев В. В. и др.** Модернизация системы диспетчерского управления движением поездов метрополитена // Тр. VIII Междунар. конф.

«Проблемы управления и моделирования в сложных системах». Самара: ИПУСС РАН, 2006. С. 269–273.

2. **Issak J., Lewis K., Thompson K., Straub R.** Open system handbook: A guide to building open systems. Piscataway: IEEE Standards Press, 1994. 197 p.
3. **Надежность в технике.** Основные понятия. Термины и определения. ГОСТ 27.002-89. М.: Изд-во стандартов, 1990.
4. **Золотухин Ю. Н., Коглер Р. Р., Михеев Ю. И.** Микропроцессорная система управления движением поездов // Метро и тоннели. 2005. № 6. С. 10–11.
5. **Белоконь С. А., Васильев В. В., Филиппов М. Н.** Программное обеспечение автоматизированной системы диспетчерского управления Новосибирского метрополитена // Тр. Седьмой междунар. конф. памяти акад. А. П. Ершова. Перспективы систем информатики. Новосибирск: Изд-во ИСИ СО РАН, 2009. С. 52–56.
6. **Филиппов М. Н.** Разработка и исследование моделей и методов построения автоматизированных систем диспетчерского управления: Автореф. дис. ... канд. техн. наук /СО РАН. ИАиЭ. Новосибирск, 2009. 18 с.
7. **Гарбук С. В., Комаров А. А., Салов Е. И.** Аналитический отчёт. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств (по материалам Интернет-изданий за 2008–2010 гг.). URL: http://www.securitylab.ru/analytics/398184.php (дата обращения: 21.03.2011).
8. **Филиппов М. Н.** Метод обработки неполных данных на основе трехзначной логики // Автометрия. 2009. **45**, № 5. С. 124–131.
9. **Белоконь С. А., Филиппов М. Н.** Метод построения многоплатформенной открытой модульной SCADA-системы // Вест. НГУ. Сер. Физика. 2008. **3**, вып. 1. С. 115–125.
10. **Филиппов М. Н.** Метод оценки надёжности программного обеспечения по информации, сохраняемой системой управления версиями // Тр. XII Междунар. конф. «Проблемы управления и моделирования в сложных системах». Самара: ИПУСС РАН, 2010. С. 244–249.
11. **Белоконь С. А., Васильев В. В., Золотухин Ю. Н. и др.** Отладка автоматизированной системы диспетчерского управления путем моделирования маршрутно-релейной централизации станции метро // Тр. Седьмой междунар. конф. памяти акад. А. П. Ершова. Перспективы систем информатики. Новосибирск: Изд-во ИСИ СО РАН, 2009. С. 48–51.
12. **Maltsev A. S., Sobolev M. A., Yan A. P.** On the question of building an open system of automated diagnostics for Novosibirsk subway // Proc. of the IASTED Intern. Conf. "Automation, Control, and Information Technology" (ACIT 2010). Anaheim — Calgary — Zurich: ACTA Press, 2010. Vol. 692. P. 174–177.

Поступила в редакцию 21 марта 2011 г.