Технические аспекты создания автоматизированных информационных систем многоцелевого применения

Орлов А.А., Рыженков С.П.
Научно-исследовательский испытательный центр «Авиационно-космической медицины и военного эргономики» 4 ЦНИИ МО РФ, г. Москва

Тельных А.А., Володин А.В., Степанов Е.А., Калюжная Н.М.
Институт прикладной физики» РАН, г. Нижний-Новгород

Сорокин А.Д.
ЗАО «РНТ» г. Москва

Аксенова Ю.Е.
МГУ им. Ломоносова

Аннотация

В современных условиях высокой вероятности возникновения чрезвычайных ситуаций в различных сферах деятельности не вызывает сомнения актуальность разработки технологии, позволяющей принимать превентивные меры при возможности возникновения угроз различного характера. Предложенные в статье подходы к созданию подобных информационных систем позволяют решать конкретные задачи обеспечения транспортной, антикриминальной, техногенной безопасности. Создание макетного образца совместно с несколькими организациями совершенно разных по виду деятельности обеспечили адекватные и универсальные решения для безопасности передачи информации, распределенного хранения, обработки и интерактивной визуализации разного типа информации.

Ключевые слова: автоматизированная информационная система; многоцелевое применение; безопасность полётов; геоинформационная система; централизованный пункт управления.

Введение

Законодателями и разработчиками автоматизированных информационных систем выступают в основном зарубежные компании (Microsoft, IBM, Oracle, Forrester): многие компоненты (протоколы обмена, системы управления базами данных, сжатие и шифрование информации) разрабатываются и производятся исключительно по патентам западных стран без предоставления исходных кодов программного обеспечения, что ставит российских разработчиков в информационную и финансовую зависимость, а также не позволяет использовать иностранные наработки в системах военного назначения. От момента создания технического задания до первого макетного образца проходит от 3-5 лет и более, за это время меняются стандарты технологий программного обеспечения: появляются новые платформы (frameworks), новые версии операционных систем, протоколы обмена данных, методы обеспечения безопасности, что ведет к тому, что результат 3-5 летней работы становится не актуальным.

Совместно с организациями (ЗАО «Российские наукоемкие технологии», «Институт прикладной физики» РАН г. Нижний Новгород, «Московский институт электронной техники» г. Москва) научно-исследовательский испытательный центр (авиационно-космической медицины и военной эргономики) 4 Центрального научно-исследовательского института Минобороны России (далее Центр) разрабатывает форсайт-проект - технологии создания автоматизированных информационных систем многоцелевого применения под общим названием «ISPLab». Для решения задач медико-технического и информационного обеспечения безопасности полетов по постановлению Правительства РФ № 307 от 2011 года на территории Центра развернута стендовая база проекта «ISPLab».

Программно-аппаратный комплекс (ПАК) «ISPLab» является технологией моделирования и проектирования комплексных систем автоматизации и управления, представляющих собой распределенные

геоинформационные системы с централизованными пунктами управления информационными потоками от различных технических систем. Данный комплекс объединяет технические системы, с наличием внешних интерфейсов взаимодействия, привязывает их к глобальным географическим координатам и трехмерным моделям местности и дает возможность интегрировать новые системы в процессе эксплуатации.

При проектировании автоматизированных систем управления и контроля ПАК «ISPLab» позволяет уточнить организационные и системотехнические решения по управлению и контролю создаваемой АИС, путем визуального моделирования местности, условий эксплуатации и параметров технических систем. Созданные, таким образом модели, могут включать в себя разрозненные технические системы – видеонаблюдение (в том числе IP-камеры и IP-серверы различных производителей), ОПС (охранно-пожарную сигнализацию), СКУД (систему контроля и управления доступом), РХБЗ (радиационная, химическая, биологическая защита) и медицинскую аппаратуру, согласованные в локальную инфраструктуру. Функциональное объединение пунктов автономного управления позволяет создать «Центр оперативного управления». При дальнейшей эксплуатации ПАК «ISPLab» обеспечивается их функционирование.

Применяемые технические решения программного обеспечения «ISPLab» могут быть использованы в различных сферах: в создании систем антикриминальной, антитеррористической безопасности, защищенных систем передачи данных видео/аудио/текстовой информации через локальные компьютерные сети или через сеть «Интернет», специальных компьютерных тренажеров, АИС безопасности полетов.

Актуальность проведения таких работ можно проиллюстрировать на примере существующей системы обеспечения безопасности полетов, созданной в 60-х годах прошлого столетия в РФ: С 1995 по 2009 год общие потери государственной авиации составили 395 воздушных судов, при этом погибли 906 человек. Относительный показатель (число авиационных происшествий на 100 тыс. часов налета), характеризующий уровень аварийности, в течение 30 лет находится на уровне 4-5 авиационных происшествий на 100 тыс. часов налета, в то время как в ведущих авиационных державах этот показатель в 2 и более раза ниже.

Технология «ISPLab» представляет собой модульное программное обеспечение, спроектированное по принципу «сверху-вниз», с возможностью расширения функционала за счет динамически подключаемых модулей и удаленного взаимодействия компонентов системы между собой. Основными компонентами, АИС являются интеграционная подсистема (ИП) и система отображения информации (СОИ).

Приведенный далее материал, представлен на примере взаимодействия интеграционной платформы с системами видеонаблюдения (IP видеокамерами), как наиболее технически сложных и требовательных к ресурсам каналов передачи данных и обработки из имеющихся современных технических систем. Представленный материал может быть адаптирован к любой другой технической системе или компьютерной программе.

Интеграционная подсистема (платформа)
Предназначение

Объединить общий функционал различных подсистем АИС, в условиях, когда этот функционал распределён между несколькими самостоятельными исполняемыми модулями программного обеспечения, а также предоставить единый программный (для разработчика) и графический (для пользователя) интерфейс.

Анализ существующих подходов

Можно выделить два основных подхода к разработке интеграционной подсистемы:

1. Каждый исполняемый модуль со своим специфическим функционалом импортирует общую интеграционную подсистему, при этом обязуется предоставить клиентскому ПО универсальный коммуникационный интерфейс.

2. Интеграционная подсистема включает первичные запускаемые программные модули, при этом она самостоятельно включает тот функционал, который экспортируется из специализированных функциональных модулей. В этом случае за коммуникацию с клиентским ПО отвечает интеграционная подсистема, а взаимодействие со специализированными функциональными модулей осуществляется исключительно через программный интерфейс.

Достоинством первого подхода является простота реализации, как общего функционала, так и модулей со своим специфическим функционалом. Данный подход более гибок с точки зрения расширения функционала.

Недостатком данного подхода является сложность реализации коммуникационной подсистемы в целом и развёртывания распределённого приложения в частности. Сложность адаптации клиентского ПО к различным коммуникационным особенностям модулей. Дублирование участков кода в различных модулях может приводить к нежелательным ошибкам в кодировании алгоритмов.

Второй подход напротив, сложнее в реализации интеграционной подсистемы, и немного сложнее в реализации модулей, при этом сильно упрощается реализация взаимодействия клиентского ПО с конечными функциональными модулями.

Архитектура подсистемы:

Проведённые исследования на макетах программного обеспечения показали преимущество второго подхода, так как он даёт больше гарантий (меньше возможностей допустить ошибки) при реализации конечного продукта.

Каждый сервис Интеграционной платформы включает в себя:

1. подсистему запуска приложения
2. подсистему поиска и загрузки специализированных функциональных модулей
3. подсистему хранения настроек специализированных функциональных модулей
4. подсистему разграничения прав доступа пользователей к функциям модулей и интеграционной подсистемы в рамках приложения
5. подсистему идентификации и аутентификации пользователей
6. подсистему межпроцессной коммуникации
7. клиентская подсистему одновременного доступа к независимым приложениям (различным процессам) с подключенными специализированными функциональными модулями.
8. Подсистему тестирования.
9. Подсистему логирования.
10. Подсистему конфигурирования (и серверной и клиентской части).

Общий алгоритм работы подсистемы

Графическая подсистема (или тестовая, или любая другая внешняя подсистема) запрашивает у клиентской подсистемы подключение к удалённым процессам, с размещёнными в них специализированными функциональными модулями.

Клиентская подсистема осуществляет подключение к удалённым процессам, и при необходимости, запрашивает аутентификацию у соответствующей подсистемы.

Клиентская подсистема предоставляет внешней (графической) подсистеме список удалённых процессов, список специализированных функциональных модулей в каждом удалённом процессе, список доступных функций в каждом модуле.

Далее клиентская подсистема осуществляет взаимодействие со специализированными функциональными модулями напрямую.

Коммуникационная подсистема может быть реализована различными способами и технологиями и быть определена при старте приложения в конфигурации приложения. Коммуникационная подсистема отвечает за целостность и доступность с точки зрения информационной безопасности на уровне интеграционной подсистемы.

Подсистема идентификации и аутентификации пользователей также может быть реализована несколькими способами.

A. Централизованная. Клиент отправляет аутентификационные данные сервису аутентификации, и получает временный идентификатор сессии. Далее, предоставляя этот идентификатор удалённым процессам с размещёнными в них специализированными функциональными модулями, интеграционная подсистема на стороне этих процессов может верифицировать этот идентификатор.

B. Распределенная. Каждый удалённый процесс осуществляет самостоятельную проверку аутентификационных данных из собственного хранилища аутентификационных данных.

В обоих случаях проверка осуществляется стандартными средствами сравнения хешей паролей, при необходимости с солью. Хранилище, содержащее аутентификационные данные, имеет стандартную структуру: логин - хеш-пароля - соль, и не зависит от конкретного провайдера СУБД.

Подсистема идентификации и аутентификации пользователей также может быть определена при старте приложения в конфигурации приложения.

При выполнении некоторой функции интеграционная подсистема обращается к подсистеме разграничения прав доступа пользователей для определения допустимости выполнения текущей операции текущим пользователем. Хранение информации о разграничении прав доступа может осуществляться различными способами: или в оперативной памяти или на файловой системе или в СУБД и определяется при старте приложения в конфигурации.

Подсистемы идентификации, и аутентификации, и разграничения прав доступа пользователей обеспечивают конфиденциальность с точки зрения информационной безопасности на уровне интеграционной подсистемы.

Серверная часть интеграционной подсистемы может быть запущена на исполнение различными способами: сервис (демон), консольное или графическое приложение.

После старта серверная часть интеграционной подсистемы осуществляет поиск и загрузку специализированных функциональных модулей и производит их инициализацию в соответствии с информацией из подсистемы хранения настроек специализированных функциональных модулей.

Подсистема хранения настроек специализированных функциональных модулей может быть реализована различными способами от файла до СУБД и определяется при старте приложения в конфигурации.

Подсистемы логирования, конфигурирования и тестирования являются обеспечивающими подсистемами.

Предложения по структуре базы данных

Интеграционная подсистема включает несколько независимых друг от друга постоянно хранимых сущностей:

Хранилище настроек специализированных функциональных модулей.

Хранилище подсистемы разграничения прав доступа.

Хранилище аутентификационных данных.

Все приведённые сущности являются тривиальными и содержат два либо три текстовых атрибута.

Аспекты информационной безопасности на уровне интеграционной подсистемы

Оценка рисков информационной безопасности выходит за рамки описания данной подсистемы, однако, учитывая то, что элементы информационной безопасности должны быть учтены на всех уровнях АИС, далее будут приведены основные тезисы.

Информационная безопасность состоит в противодействии реализации следующих угроз:

1. Угроза нарушения конфиденциальности информации (НСД)
2. Угроза нарушения доступности информации (отказ в обслуживании)
3. Угроза нарушения целостности информации (изменение информации)

Стоит отметить, что реализация противодействия всем угрозам одновременно не возможна – необходимо ранжировать угрозы и на этой основе сбалансировать меры информационной безопасности.

Выявить риски и ранжировать эти угрозы по значимости – не простая задача. Ведь, например, злоумышленник может получить доступ на просмотр видеоизображения некоторой камеры. Это однозначно нехорошая ситуация. Однако если злоумышленник не может получить права на просмотр камеры, то он может попытаться загрузить её большим числом подключений, и в результате она выключится. Пока дежурный будет предпринимать меры по устранению неисправности, картинки с камеры некоторое время не будет (изображение с камеры будет отсутствовать). И последний пример нарушения целостности информации – если злоумышленник не может воздействовать на оборудование, но имеет возможность физически (или логически через маршрутизатор) встать в разрыв соединения, то он сможет транслировать записанный ранее видеопоток.

Таким образом, при разработке интеграционной подсистемы, необходимо учесть все угрозы информационной безопасности.

Общий подход к обеспечению информационной безопасности заключается в том, что если злоумышленник реализовал угрозу для одного из элементов системы, то это не должно сказаться на других элементах. Например, если злоумышленник смог проникнуть в систему с установленным сервисом АИС, то он не должен получить доступ на все сервисы системы.

Предлагается:

- Хранить пароли для сервисов по отдельности либо сервисы должны иметь только право проверки хешей паролей из центрального хранилища
- Реализовать шифрование и цифровую подпись сообщений в коммуникационной подсистеме.
- Все программные средства системы (сервисы, подключаемые модули и клиенты) должны иметь цифровую подпись (или подписанный сертификат). Сервисы и клиенты не должны загружать неверифицированные модули. Клиенты не должны подключаться к неверифицированным серверам.
- Для защиты от атак отказа в обслуживании настроить сетевое оборудование, использовать средства сетевого мониторинга, для объёмного трафика использовать специализированные протоколы
- Использовать антивирусные средства, IDS

Интеграционная подсистема с точки зрения специализированных функциональных модулей

Хотя интеграционная подсистема является прозрачной для внешней (графической) подсистемы, она накладывает ограничения на интерфейс специализированных функциональных модулей.

Концепция интерфейса специализированного функционального модуля заключается в наличие нескольких служебных и двух основных элементов.

1. Абстрактная операция специализированного функционального модуля.
2. Абстрактное событие специализированного функционального модуля.

Вся функциональная логика модуля проходит исключительно через эти два элемента.

Абстрактная операция – это некоторое действие (из заранее определённого набора операций модуля), которое имеет идентификатор, абстрактный аргумент и абстрактное возвращаемое значение. Тип (или даже наличие) аргумента и возвращаемого значения определяются исходя из типа (идентификатора) операции. Операция может также завершится неудачей (например, нет прав доступа) – тогда вместо возвращаемого значения клиент получит соответствующую ошибку.

Стоит обратить внимание, что все операции являются БЛОКИРУЩИМИ. Это с одной стороны упрощает клиент – там нет необходимости «вручную» ждать завершение или ошибку операции, с другой стороны появляется необходимость добавлять асинхронность к элементам графической подсистемы. Достоинством данного подхода по сравнению с асинхронной моделью операций является простота определения соответствия, какая операция завершилась, каков её результат и в какой операции произошла ошибка.

Данное свойство операций накладывает дополнительное ограничение на коммуникационную подсистему. Так как операция специализированного функционального модуля является блокирующей, коммуникационная система должна организовывать на каждую операцию новый свободный канал межпроцессной коммуникации. (При этом не обязательно каждый раз создавать канал заново – возможно использовать пул каналов.)

Абстрактное событие – это некоторая информация, которую специализированный функциональный модуль может предоставить клиентам по собственной инициативе. При этом кому из клиентов будет передано событие, определяется в подсистеме интеграции на основе заявок клиентов и матрицы прав доступа.

Поскольку событие инициируется на стороне сервера, клиент не может знать о передающемся в канале событии. И поэтому не может создать для каждого события отдельный канал. При этом события по своей природе являются асинхронными – специализированному функциональному модулю нет необходимости ждать пока клиенты обработают и отреагируют на событие, своего рода уведомление. В связи с этим интеграционная подсистема всегда выделяет под события один свободный канал на одного клиента. А сами события должны быть как можно более легковесными, чтобы отправлять таких сообщений как можно больше в единицу времени.

Интеграционная подсистема с точки зрения видеообработки

Приведённая модель распределённого взаимодействия является оптимальной с точки зрения масштабирования и гибкости создания специализированных функциональных модулей и простоты интеграции в единую систему в условиях повышенных требований информационной безопасности.

Однако и недостатки у этой модели тоже присутствуют. Главный недостаток это повышенное потребление ресурсов ЭВМ подсистемой коммуникации – это цена за гибкость протокола и использование криптографических средств защиты.

Но в большинстве случаев - эта особенность недостатком не является в виду отсутствия большой нагрузки (большинство операций и событий не велики по размеру).

Исключением является трафик мультимедиа контента и видеопотока в частности. Профилирование макета показало, что узким местом при трансляции видеопотока является именно коммуникационная подсистема. Ситуация, когда каждый видеокадр сопровождается дополнительным ненужным в данном случае объёмом информации, отрицательно влияет на качество передаваемого сигнала и производительность всей системы. К тому же универсальные и гибкие средства коммуникации не очень хорошо приспособлены для передачи видео реального времени, особенно нескольким клиентам одновременно. Стандартное число параллельных подключений на один сервер общего назначения равняется 10.

В связи с этим предлагается применить наработки в области широковещательной трансляции видеопотока по специализированным протоколам. Особенность данного протокола в том, что видео сервер посылает только один ip-пакет, в котором указан список адресов-получателей. При этом трафик сервера падает в N раз (N – количество клиентов), а трафик маршрутизатора уменьшается в 2 раза – маршрутизатор собственно и осуществляет копирование пакетов.

Таким образом, клиент будет устанавливать два соединения: первый сигнальный канал через интеграционную систему и второй параллельный канал через multicast-протокол для приёма видеосигнала.

Для унификации видео-протокола предлагается следующий подход.

Специализированный функциональный модуль, который собирается транслировать видеосигнал, запускает сервер видео (ре)трансляции, который предоставляет интеграционная инфраструктура. Этот сервер передаёт видео поток в настраиваемом, но стандартизованном виде. Поэтому, клиенты могут к нему подключиться без проблем. С другой стороны специализированный функциональный модуль может подключиться к источнику видео любого формата, перекодировать этот сигнал в стандартный формат, после чего и производить ретрансляцию.

Таким образом, обеспечивается согласование форматов стандартного клиента и некоторого нестандартного устройства на уровне специализированного функционального модуля.

Нельзя не отметить, что данный метод организации связи является дополнительно трудоёмким с точки зрения настройки сетевой инфраструктуры, в особенности настройки сетевых экранов.

Однако применение данных технологий способно дать большой выигрыш в производительности системы и в качестве видеосигнала.

Подсистема отображения информации
Описание подсистемы отображения информации

Подсистема отображения представляет собой клиентское приложение для конфигурирования и контроля работы интеграционной платформы в конкретных условиях эксплуатации.

Подсистема отображения информации представляет собой графическую прикладную программу, предназначенную для визуализации потока технической информации, поступающего из системы распределенных сервисов интеграционной платформы. Данная система декодирует поток событий технических систем (видео аналитики и др.) в поток элементов изображения на экран в виде динамического цифрового макета объекта управления.

Система включает средства фильтрования потока элементов изображения с помощью системы глобального позиционирования (Global Positioning System) на экране пользователя и систему вычисления трехмерного изображения. В результате совместной работы двух систем каждый декодированный элемент потока технической информации визуализируется как элементарное трехмерное изображение с точным позиционированием и масштабированием относительно контролируемого участка местности (GPS- rectangle).

Техническим результатом является минимизация объема передаваемого трафика, например, от систем видеонаблюдения за счет представления видеоинформации как событий обычной технической системы на цифровом макете объекта.

Предложения по структуре подсистемы

- Клиентская подсистема
- система анализа информационных моделей
- средства фильтрования потока элементов
- система вычисления трехмерного изображения
- система отображения

Общий алгоритм работы подсистемы

Клиентская подсистема запрашивает у сервиса аутентификации список разрешенных текущему пользователю подключений к удалённым сервисам интеграционной платформы.

Клиентская подсистема осуществляет подключение к разрешенным удалённым процессам, и при необходимости, запрашивает аутентификацию.

Клиентская подсистема предоставляет Системе анализа информационных моделей список удалённых процессов, список специализированных функциональных модулей в каждом удалённом процессе, список доступных функций в каждом модуле.

Далее клиентская подсистема осуществляет взаимодействие со специализированными функциональными модулями по установленному протоколу обмена.

Система отображения с помощью конвекторов переводит техническую информацию в трехмерное графическое изображение на цифровой карте мире.

Предложения по структуре базы данных

Использование баз данных в Системе отображения не принципиально, так как все команды и события логируется на уровне информационных сервисов.

Детализированный перечень функций подсистемы

Основные функции Подсистемы отображения информации:

- Подключение к интеграционной платформе системы и загрузка его конфигурации – выполняется с помощью клиентских команд.
- Отображения (Отображение) дерева объектов информационных модулей.

- Отображение визуализаторов устройств и цифровых объектов в главной форме приложения, а также в дополнительных по требованию пользователя.
- Отображение карты мира с расположенными на ней устройствами и цифровых 3d объектов.
- Масштабирование визуализаторов в зависимости от текущего масштаба карты.
- Сохранение и загрузка конфигурации открытых визуализаторов – расположение открытых визуализаторов можно сохранить для того, чтобы при повторном открытии приложения они были автоматически открыты.
- Создание и выполнение сценариев (системы помощи принятия решения).
- Объединение визуализаторов в логические группы и передача групповых событий между визуализаторами (например, обмен сообщениями между пользователями).
- Контроль действий пользователя и отмена их.

Предложения по сценариям представления информации

Для отображения сценариев представления информации представляется модуль математической модели, который предназначен для обеспечения взаимодействия устройств, зарегистрированных в службах информационных моделей устройств. Визуальным отображением модуля математической модели является трехмерное пространство с наложенным на нижнюю плоскость сетки (далее - IGrid). Данная сетка, учитывая географическую привязку, позволяет суммировать информационные модели устройств, а также данные, получаемые от системы видеоаналитики, в виде графической информации (трехмерные модели новых объектов на сцене, выделять из них «интересных») на фоне 3D-архитектуры контролируемого объекта/местности. Также модуль обеспечивает создание сценариев, которые строятся на основе диаграмм последовательностей. Сценарии могут быть использованы для автоматического управления оборудованием в зависимости от текущего состояние всей системы и использованы для поддержки принятия решения оператором.

Для расширения управляющих и вычислительных возможностей сценариев предполагается обеспечить возможность подключения сложных правил, различных видов математической обработки на основе формул Бернулли, Лапласа и др. В качестве инструмента для создания данного расширения в интеграционной платформе предлагается использовать библиотеку .Net Framework на Windows NT, Mono на OS Linux, и непосредственно такую возможность, как динамическую компиляцию кода, написанного на языке C# / или JavaScript.

Данный модуль позволяет генерировать события срабатывания датчиков от технических характеристик используемых сенсоров (видеокамер), например, характеристик пассажиропотока (плотность, скорость движения), особенностей условий эксплуатации, для тестирования работы ПО в целом.

Модуль визуализации математической модели

Данный модуль предназначен для визуализации информационных моделей устройств, входящих в математическую модель. Модуль имеет двунаправленный канал подключения к службе математической модели, что обеспечивает двустороннюю связь. Модуль математической модели, обрабатывая системную информацию от всех типов устройств, генерирует «тревожные события» с указанием пространственных координат, просчитывает такие показатели как вероятность ложного сигнала, вероятность отказа оборудования, визуализирует состояния устройств. Кроме того, модуль визуализации математической модели за счет двунаправленных каналов подключения позволяет вносить необходимые корректировки в работу модуля математической модели (обучать модуль дополнительным условиям функционирования).

Архитектура данной системы также позволяет создавать каналы подключения между службами представления, это может быть использовано для самообучения других модулей системы, в случае если при одних и тех же условиях определенный опыт повторяется n раз и если вероятность того, что события A в серии из n опытов произойдет ровно k раз, может быть применена формула Бернулли.

Отображение математической модели происходит на специальной форме FormMap, которая содержит цифровую карту мира и позволяет вычислять глобальные координаты каждого из объектов, привязанных к IGrid, и одновременно просматривать другие математические модели.

Состав и функции компонентов подсистемы
Клиентская подсистема

Клиентская подсистема – представляет собой сервис, которая реализует CallBack интерфейс интеграционной платформы. Клиентская подсистема предназначена для функций конфигурирования, настройки устройств; работы с уровнями доступа и передачи служебной и сервисной информации.

Работа клиентов через данный интерфейс выполняется в следующей последовательности:

Connect – подключение пользователя с указанием имени пользователя;

- Выбор (Выбора) типа устройства;
- Выбора устройства;
- Подписки на события

Клиентская часть подключения к СПМ Сервису строиться на базе автоматически формируемого файла описания интерфейса (XML). Данный класс имеет набор методов, реализующих интерфейс и обратное событие. Таким образом, события, происходящие в интеграционной платформе, будут доставляться клиенту.

Класс имеет специальный поток контроля соединения с интеграционной платформой. При разрыве или ошибке связи происходит автоматическая попытка переподключения клиента к интеграционной платформой (платформе).

Система анализа информационных моделей

Данный модуль оперирует информационными моделями изображений видеокамер «цифрой моделью устройства» (далее - устройство).

Описание устройства определяет характеристики устройства, значение состояния (параметры, характеризующие работу устройства – например, текущее состояние устройства или найденные объекты на видеоизображении), родительское устройство (например, группу), набор подчиненных устройств.

При загрузке сервиса все устройства производят подключение к интеграционной платформе, на которой они зарегистрированы. С помощью TCP\IP канала происходит всё взаимодействие системы визуализации и Сервиса Информационной модели для конкретного устройства – обновление статуса устройства, получение событий, вызов команд и т.п. Происходит загрузка системных событий и команд, которые зарегистрированы в Сервисе, и объединение с системными событиями и командами, прочитанными при загрузке из файла конфигурации устройства.

Все поступающие системные события от Сервиса анализируются и кладутся в очередь событий для последующей передачи клиенту. Анализ события производится в зависимости от типа события и в очередь событий устройства добавляется соответствующая запись. Впоследствии, в специальном потоке происходит проверка всех устройств на наличие событий в очереди, анализ события и соответствующая обработка.

Аналогично происходит формирование системных событий: событие кладется в очередь событий клиентов, в потоке контроля соединения клиента очередь проверяется, и событие отправляется Системе визуализации.

Устройства могут быть объединены в группы. Группа определяет устройства, которые включены в данную группу. Они могут быть двух типов – отдельно сконфигурированное устройство, или уже созданная группа устройств. На стороне клиента для построения дерева требуется загрузить все устройства и группы, пройтись по всем группам, рекурсивно построить дерево объектов исходя из массива объектов, которые находятся в конкретной группе.

Права доступа к группам устройств делегируются по правилам интеграционной платформы.

Для устройства настраиваются элементы отображения в зависимости от вариантов состояния устройства. Для каждого состояния имеется возможность задать графический ресурс (пиктограмму) и звуковой файл. Звуковой файл проигрывается при переходе из одного состояния в другое.

Средства фильтрования потока элементов

Средства фильтрования потока элементов представляют собой коллекцию конвертеров, осуществляющих подготовку информационных моделей.

В информационные модели передаются значения определяющие видимость, позицию на карте, цветовое отображения состояния, информационные проекции объектов на видео изображении. При каждом изменении свойства модели генерируется событие для системы вычисления трехмерного изображения и поток элементов изображения передается далее.

Система вычисления трехмерного изображения

Система вычисления трехмерного изображения обеспечивает надежное и адаптивное отображение объектов любого вида из потока информационных моделей. Главной задачей системы является кодирование системы выведения на экран цифрового макета объекта в виде синтезированного 3D-изображения, в котором поток динамической информации сужается при помощи специфического кодирования, что позволяет также существенно улучшить непрерывность выведения на экран 3D-изображения.

Система вычисления трехмерного изображения предназначена для получения обработки потока элементов изображения, который включает адресуемые элементы изображения, каждый из которых образован геометрической формой, согласно действующим правилам системы видео аналитики.

В зависимости от информации, заложенной в информационной модели, система вычисления трехмерного изображения создает графический трехмерный объект. Например, если с модуля видеоаналитики пришло событие о появлении нового человека, данная система создаст 3d модель человека с его отличительными признаками.

Система отображения

Главной целью Подсистемы отображения является скорость визуализации. Чтобы обеспечить своевременное отображение сложных текстур, специальных эффектов вроде частичной прозрачности и трехмерной графики. Прорисовка сложной трехмерной графики (DirectX's forte) проходит через конвейер DirectX, который включает поддержку всех современных видеокарт. DirectX передает как можно больше работы узлу обработки графики (graphics processing unit - GPU), который представляет собой отдельный процессор на видеокарте. Кроме того, система отображения базирует свое масштабирование на системной установке DPI, а не на DPI физического дисплейного устройства. Это значит, что любое отображение (включая фигуры, элементы управления, текст и любые другие ингредиенты, которые помещаются в окно приложения) на 100-дюймовом проекторе или видеостене, будет выглядеть также как на 17 дюймовом мониторе.

Система отображения предназначена для окончательного синтеза всей графической информации, имеющейся в памяти программы, для вывода ее на экран пользователя. Данный процесс осуществляется следующим образом: информационные модели в виде синтезированного трехмерного изображения макета объекта, выдаваемым прикладным модулем видеоаналитики, поступают в Систему отображения, из потока выделяются элементарные изображения, образующие часть выводимого на экран синтезированного трехмерного изображения.

Характеристика информационных связей между компонентами подсистемы и алгоритм работы подсистемы с привязкой к компонентам подсистемы

Для создания подсистемы отображения информации была выбрана технология под названием «модель-представление-модель представления Model–View – ViewModel». Данный шаблон проектирования применительно к сочетанию трехмерной графики и двумерной графики в Системе отображения

позволяет создавать только один экземпляр класса объекта информационной модели устройства-видеокамеры, что значительно экономит системные ресурсы видеокарты с одной стороны и – обеспечивает синхронное отображение видеоинформации во всех модулях системы.

Информационные связи между компонентами подсистемы осуществляются с помощью технологии Binding. В своей простейшей форме привязка данных - это отношение, которое сообщает Системе отображения о необходимости извлечения некоторой информации из исходного объекта и использования его для установки свойства в целевом объекте. Конечной целью привязки данных является отображение некоторой информации в пользовательском интерфейсе. Объектом-источником может быть другая информационная модель или конкретный метод клиентского модуля.

Для вызова команд из пользовательского интерфейса используется очередь задач, которая проверяет на ошибку действие пользователя. Все активные элементы приложения подключают элементы управления к ним, тем самым избегая необходимости писать повторяющийся код для обработки событий. Эти задачи могут инициироваться различными действиями и через различные элементы пользовательского интерфейса, включая главные меню, контекстные меню, клавиатурные комбинации и панели инструментов. Функция команд управляет состоянием пользовательского интерфейса, автоматически отключая элементы управления, когда связанные команды не доступны. Она также предоставляет центральное место для хранения (и локализации) текстовых заголовков команд.

Также в классе задач может быть реализован, журнал хронологии команд и поддержка для используемой на уровне приложения функции Undo, и создание системы для отслеживания и аннулирования команд.

Заключение

Разработана технология «ISPLab», позволяющая:

- создавать автоматизированные информационные системы многоцелевого применения;
- обеспечивать работу высоконагруженных распределенных информационных систем в АИС;
- интегрировать различное техническое оборудование и обеспечивать прием обработку и передачу технической информации;
- интерактивно отображать в трехмерном представлении, на цифровой карте мира различного рада информацию в виде пиктограмм, графиков, анимированных объектов во взаимосвязи с глобальными координатами;
- изменять и расширять функционал без перепроектирования АИС в целом;
- разворачивать интеграционную подсистему на различных операционных системах Linux/Windows.

Литература

1. РД 5Р.8713-93. Аппаратура радиосвязи и радиолокации. Методы оценки электромагнитных полей и средства защиты личного состава судов от облучения.

2. ОСТ 5Р.6186-2005. Нефтеналивные суда и нефтепричалы. Электростатическая и гальваническая искробезопасность. Общие технические требования.

Для цитирования:

Орлов А.А., Рыженков С.П., Тельных А.А., Володин А.В., Степанов Е.А., Калюжная Н.М., Сорокин А.Д., Аксенова Ю.Е. Технические аспекты создания автоматизированных информационных систем многоцелевого применения // i–methods. 2013. Т.5. №2. С.22–34.

Technical aspects of creation of automated information systems multi-purpose applications

Orlov A.A., Ryzhenkov S.P.
Scientific-research test center of "aerospace medicine and military ergonomics" 4 TSNII MO RF, Moscow

Tel'nyh A.A., Volodin A.V., Stepanov E.A., Kalyuzhnaya N.M.
Institute of applied physics" RAS Nizhny Novgorod

Sorokin A. D.
JSC "RNT", Moscow

Aksenova Yu.E.
MSU Lomonosov

Abstract
In modern conditions a high probability of occurrence of emergency situations in various spheres of activity is no doubt about the urgency of developing a technology that enables to take preventive measures when the possibility of threats of various kinds. The approaches to this article of such information systems enable to solve the specific challenges of providing transport, anti-crime, industrial security. The creationf of the model sample, together with several organizations are quite different in type of activity provided adequate and universal solution for the security of information transfer, distributed storage, processing and interactive visualization different types of information.

Keywords: threat; Information security; border area; the accuracy of the display; coverage.

References
1. RD 5P.8713-93. Equipment of radio communication and radar systems. Evaluation methods of electromagnetic fields and protection of personnel from radiation vessels.
2. OST 5P.6186-2005. Oil tankers and accomplished a bulk oil terminals. Electrostatic and galvanic isolation intrinsic safety. General technical requirements.

For citation:
Orlov A.A., Ryzhenkov S.P. Tel'nyh A.A., Volodin A.V., Stepanov E.A., Kalyuzhnaya N.M., Sorokin A.D., Aksenova Yu.E. Technical aspects of creation of automated information systems multi-purpose applications // i-methods. 2013. T. 5. No. 2. Pp. 22-34.