Общество с ограниченной ответственностью «ЭкспертСтройПроект»
ОГРН 1115042001030, ИНН 5042117602

Инструкция по установке и эксплуатации (пользовательская инструкция) для программы ВРА2 -9.1

СОДЕРЖАНИЕ

1. Введение

Данный документ является кратким руководством по эксплуатации продукта БПА2 (ВРА-9.1), входящего в состав МРС2 и не используется обособленно и отдельно.

Пожалуйста, внимательно изучите весь документ перед использованием информации, представленной в нем, для выполнения любых действий в рамках системы.

Гарантия будет аннулирована в случае, если персонал, кроме специально обученного и квалифицированного персонала, будет распаковывать, обращаться, устанавливать, монтировать, настраивать или вводить в эксплуатацию систему или системные модули.

Центральная система централизации включает в себя:

- Ethernet-коммутатор для внутренней связи
- два безопасных процессорных устройства (компьютеры A и B) для безопасной обработки данных, с LAN-контроллерами для внутренней связи
- сервисное процессорное устройство (компьютер C) для выполнения обработки, не влияющей на безопасность системы, с LAN-контроллерами для внешней /внутренней связи

1.1 Терминология

МПЦ-ЭЛ- Микропроцессорная централизация, типовое изделие

МПЦ - Центральная система централизации

OCLOOP - Преобразователь петли Ethernet

MPC2 - Процессорный блок централизации, типовое изделие

LAN - Локальная вычислительная сеть (ЛВС)

РБЦ - Радио блок-центр

ДЦ - Система управлением движением

TABS - Точка доступа к службам транспортного уровня

MPU - Критически важная виртуальная платформа

ILS - Приложение по централизации

NV - Постоянный

Система ОК - Система объектных контроллеров

КВП - Компьютер виртуальной платформы

ИКС - Интерфейс командной строки

IEP - Процесс проектирования централизации

RACP - платформа центрального процессора МПЦ, использующая процессор Эльбрус

Приложение централизации - GP, GA и SA вместе образуют приложение централизации

Резервирование - Техника разработки, при которой используется дополнительное резервное оборудование одного типа

1.2 О программе

Данная программа БПА2 предназначена для работы в качестве безопасного модуля «Б» диверсифицированной системы MPC2.

При развертывании, приложение централизации исполняется в двух экземплярах

- Один экземпляр в режиме онлайн
- Один экземпляр в режиме резервирования.

Эти экземпляры исполняются в рамках резервированной архитектуры аппаратных средств.

Во время исполнения система автоматически решает, какая из двух систем переходит в режим онлайн, а какая – в режим резервирования.

Приложение централизации устанавливается на обеих системах, поэтому Вам потребуется повторить инструкции по установке и обновлению, содержащиеся в этом документе, для системы 1 и системы 2.

Приложение централизации поддерживает три различные целевые системы

- MPU
- RACP
- Одиночный ПК (SinglePC)

Где целевые объекты MPU и RACP используются в рамках коммерческой эксплуатации, а одиночный ПК является целевым объектом для функциональных тестов.

Целевой одиночный ПК работает только в нерезервированной конфигурации.

Перекрёстное сравнение осуществляется в течение заданного периода времени. По истечении временного периода система останавливает работу. Обнаружение ошибок должно происходить насколько возможно быстро. Временной интервал перекрестного сравнения задается в параметрах конфигурации.

Перекрестное сравнение гарантировано для следующей информации:

- источник

- получатель

- последовательность

- время

Ошибки процесса перекрестного сравнения останавливают работу системы.

Информация, использованная для перекрестного сравнения, уничтожается по завершении перекрестного сравнения, из-за необходимости предотвращения повтора перекрестного сравнения одной и той же информации.

Системе присваивается уникальное наименование. Наименование определено в файле данных приложения.

Правильность адреса обеспечивается на этапе проектирования системы, так же осуществляется выдача аварийного сигнала.

Система не включается в работу без наличия надлежащих программных файлов, поэтому проверка степени защиты загруженных ПО-модулей проводится до момента начала обычной работы системы. Поставляемые артефакты продукта FVSP2, а именно: исполнимые модули и библиотеки, в случае их установки на целевой платформе, четко отделяются от файлов данных приложения.

Обеспечивается возможность исполнения FVSP2 без проверки аппаратных средств или управления временем. Это необходимо для обеспечения возможности контроля системы на базе функций ПК или сервера с низкой скоростью или занятыми другими процессами.

1.3 Функции ввода-вывода

1.3.1 Интерфейс логики централизации

FVSP2 информирует логику централизации об изменениях системного режима. В качестве таковых переменных заданы следующие значения:

1) набор инструкций к запуску
2) набор инструкций на случай переключения до завершения процесса обновления из режима ожидания в интерактивный режим
3) набор инструкций на случай переключения из режима ожидания по завершении процесса обновления в интерактивный режим

1.3.2 Обработка интерфейса объектов контроллера ввода

Данная функция обеспечивает обработку интерфейса ввода на маршруте к контроллеру.

Т.е. это дополнительный модуль, преобразующий текущее состояние объекта в формат, используемый FVSP2. FVSP2 также обеспечивает обработку коммуникации в направлении к или от ОС при помощи WSL. В этом случае внутренний дополнительный модуль используется для сопряжения FVSP2 и WSL.

Для считывания статуса объектных контроллеров, подключенных к напольным объектам, проводится упорядоченный опрос объектов контроллера в рамках каждого цикла. Интерфейс обеспечивает обработку, как уровня защиты, так и прикладных подсистем (распаковка и распределение информации)

Так же FVSP2 осуществляет коммуникацию с ПО, как внутреннего, так и внешнего YCU одновременно.

При обнаружении FVSP2 сообщения некорректной длины (ML) или некорректного типа команды (CO), система сбрасывает остаток сообщения о статусе объектного контроллера, подключенного к напольным объектам, превышающее нормативную длину сообщения.

2. Процедура инсталляции ПО

Это продукт при компиляции пакета логики включаются в общий пакет и инсталлируется вместе с пакетом логики, никогда отдельно.

2.1 Установка прикладного пакета логики взаимозависимостей станции.

Для установки пакета ILS в первую очередь необходимо скопировать инсталляционный пакет продукта ILS на машину C (CA) платформы RACP.

Установка и удаление прикладного пакета логики взаимозависимостей осуществляется только на машинах C (CA) основной и резервной

половины ЦП, машины A и B запускают соответствующие модули скопировав их по локальной сети с машины C при старте комплекса.

2.2 Удаление ранее установленного пакета логики

Если на машине C (CA) уже установлен пакет ILS, следует его деинсталлировать следующими командами:

systemctl stop vpu /etc/software/ils.remove

Если установлен пакет ilstest, его также необходимо удалить командой:

/etc/software/ilstest_target.remove

2.3 Установка нового пакета логики

На машине C (CA) перейти в каталог, в который скопирован инсталляционный пакет взаимозависимостей, и выполнить команду:

bash ils.ILS2_RF_VLADIK-2.4R.setup

где ILS2_RF_VLADIK-2.4R — название пакета логики.

В процессе установки выберите продолжение установки (y) и подтвердите, что платформа установки действительно RACP.

This is the setup for:

Product : ILS2_RF_VLADIK-2.4R

Product number : RUSIG0003

Creation time : 2017-09-26 15:28:10

Platform : RACP Do you want to continue [y/N]:

3. Техническое обслуживание

3.1 Общие положения

Во время проведения технического обслуживания принимаются надлежащие меры безопасности с целью:

- обеспечения безопасности движения

- обеспечения, по мере необходимости, отключения оборудования от сети, во избежание нанесения травм персоналу и повреждения оборудования

- предотвращения поражения электростатическим разрядом при эксплуатации электронного оборудования

3.2 Диагностика

Терминал технического обслуживания – это программное приложение для обслуживания и диагностики, которое обеспечивает доступ к информации, содержащейся на жестком диске компьютера C, например, к системным журналам и документации устройства.

Компьютер, на котором выполняется приложение обслуживания и диагностики, подключается к центральной системе централизации либо удаленно через сеть, либо локально к Ethernet-коммутатору центральной системе централизации.

4. Внеплановое техническое обслуживание

4.1 Обновление программного обеспечения

Операционная система, прикладное программное обеспечение для компьютеров A, B и C обновляется как часть работ по техническому обслуживанию, выполняемых уполномоченным персоналом по техническому обслуживанию.

4.2 Замена оборудования

Замена оборудования производится аттестованным ремонтно-обслуживающим персоналом. Эти действия включают следующие шаги:

- локализация и проверка неисправности или замена элемента
- демонтаж оборудования
- установка запчасти на демонтированное оборудование

- подключение вновь установленного оборудования к заземляющему устройству и электросети
- подача питания на вновь установленное оборудование
- настройка оборудования, при необходимости
- проверка оборудования при нормальном режиме работы

При подаче питания на компьютеры A, B и C происходит автоматическая загрузка операционных систем и прикладного программного обеспечения.

5. Ограничения конфигурации МПЦ

5.1 Безопасность

Все прикладные условия обеспечения функций безопасности (SRAC) MPC2, обеспечиваются типовым применением MPC2.

5.2 Общие положения

В этом разделе представлены ограничения конфигурации для центральной системы централизации. Представлены системные ограничения.

Поддерживаемая МПЦ продолжительность цикла составляет 600 мс. Это ограничение обусловлено использованием подсистем, не поддерживающих более короткие значения времени цикла.

5.3 Подключение Системы управления движением (ДЦ)

МПЦ обрабатывает до 20 идентификаторов ДЦ. Однако это зависит от применяемых государственных железнодорожных стандартов и используемой версии ДЦ Plug-in. Фактическое количество подключений ДЦ указано в документации ДЦ Plug-in.

5.4 Связь с централизацией и одноранговыми РБЦ

МПЦ выполняет до 8 подключений к централизации/ или одноранговым РБЦ с резервированием на уровне сети и машины.

За цикл связи (600 мс) на один одноранговый узел отправляется до 8 телеграмм. В зависимости от размера определенных объектов, это позволяет менять состояние приблизительно 400 - 600 активным объ-

ектам одного однорангового узла связи. Обратите внимание, что количество объектов, определенных для замены, может быть больше, но только активные объекты могут поменять свое состояние.

Кроме того, необходимо проверить, что теоретическая пропускная способность сети, фактическая пропускная способность сети и объем данных объекта, которые должны быть переданы между одноранговыми узлами, удовлетворяют следующему требованию:

$$\text{Пропускная способность сети} > \frac{\text{MSS}}{\text{RTT}} \times \frac{\text{C}}{\sqrt{\text{p}}} > \text{Tg} \times \text{Ts} \times \text{Ti} \times \text{Ct}$$

Фактическая пропускная способность сети:

MSS - максимальный размер сегмента в байтах (обычно 1460 байт)

RTT – время на передачу и подтверждение, с

p – интенсивность потери пакетов

C – константа, равная единице

Пропускная способность сети, необходимая для передачи данных объекта

Tg – количество телеграмм

Ts – размер телеграммы в байтах (включая телеграмму A и B)

Ti – количество TABS, участвующих в создании телеграммы

Ct – константа, равная 1,67, из расчета времени цикла 0,6 с

5.5 Подключение к терминалу обслуживания

Для центрального или резервного МПЦ отсутствуют ограничения на количество подключений к терминалу обслуживания.

Однако обратите внимание, что центрального или резервного МПЦ разрешено устанавливать только одно соединение с доступом для чтения/записи. Отсутствуют ограничения на соединение с доступом только для чтения.

Разрешения на чтение или запись зарезервированы для учетной записи пользователя «техник», в то время как доступ только для чтения зарезервирован для учетной записи пользователя «читатель».

5.6 Ограничения концепции передачи

На участке эксплуатации железной дороги, использующем объектный контроллер типа OCS950, используется адрес концентратора 0x00. Все концентраторы, используемые на участке, настраиваются подобным образом.

5.7 Ограничения логической централизации объектов

Доступны две конфигурации МПЦ со следующими ограничениями использования логических объектов для логики централизации:

- МПЦ для нормальных условий окружающей среды способна обрабатывать до 3000 логических объектов

- МПЦ для экстремальных условий окружающей среды способна обрабатывать до 500 логических объектов.

Вышеупомянутые ограничения функционально безопасны при времени цикла 600 мс.

5.8 Буферы связи объектных контроллеров, подключенных к напольным объектам

В редких случаях на длинных участках железной дороги из-за буферов UDP, размещенных на сервисном компьютере С, в МПЦ, при попытке прочтения, теряются телеграммы резервных объектных контроллеров.

Чтобы настроить буферы на размер станции, выполняются следующие действия:

- Убедитесь в отсутствии пакетов на резервном компьютере с помощью команды "netstat –su". Ищите «ошибки приема пакетов» в распечатке в разделе UDP. С помощью команды "sysctl net.core.rmem_max" получите значение размера буфера, присеваемое по умолчанию. Запишите полученное значение размера буфера.

- Измените размер буфера с помощью "sysctl -net.core.rmem_max=new_value" и "sysctl -w net.core.rme_default = new_value". Если значения добавить в /etc/sysctl.conf, они не изменяться после перезагрузки системы. Заметьте, что new_value – это новый увеличенный размер буфера.
- Убедитесь в наличии пакетов на резервном компьютере с помощью команды "netstat –su". Если пакеты по-прежнему теряются, повторите предыдущее действие и попытайтесь постепенно увеличить размер буфера до тех пор, пока ни один пакет не будет утерян.

5.9 Ограничения OCLOOP OCS 950

При подключении МПЦ через OCLOOP к петле объектного контроллера типа OCS 950 необходимо использовать карту концентратора типа ROF1373013/104.

6. Проектирование архитектуры

6.1 Общие сведения

Программное обеспечение MPC2 содержит три подсистемы: БПА2, БПВ2 и VSP2.

Подсистемы БПА2 и БПВ2 имеют независимое планирование, при котором функции выполняются в цикле.

Функции в VSP2 управляются событиями. Некоторые из них основаны на типе взаимоотношений «клиент-сервер», а другие взаимодействуют с БПА2 и БПВ2 в режиме задач обмена данными.

BPPDA2/TABSA2TCP и BPPDB2/TABSB2TCP являются собственными разработками, которые выполняются в процессе БПА2 и БПВ2. Они управляются событиями по вызовам API из БПА2 и БПВ2.

6.1.1 Обзор

Подсистемы MPC2 — БПА2, БПВ2 и VSP2 — выполняются на трех отдельных платах ЦП, обозначенных как A, B, C. Для резервирования предусмотрено два набора плат ЦП. Между ними находится замкнутая сеть и дополнительное соединение между ЦП платы C. Сеть представляет собой Ethernet, где коллизии устраняются с помощью дуп-

лексной структуры. Каждая плата ЦП-С управляет энергонезависимым запоминающим устройством.

Платформа MPU содержит аппаратное обеспечение и операционные системы. Эта платформа нс основе COTS спроектирована таким образом, что она соответствует концепции безопасности. Для БПА2 и БПВ2 предусмотрены разные ЦП, платы ЦП и операционные системы, чтобы обеспечить разнотипность на всех этих уровнях.

Подсистемы БПА2 и БПВ2 реализуют функции безопасности разнотипно. Адаптация этих подсистем обеспечивается путем блокировки логики, и эти подсистемы также зависят от данных участка эксплуатации ж. д. Файлы логики блокировки (GA) и данных участка эксплуатации ж. д. (SA) рассылаются в место назначения пакетами, которые можно легко обновить и отдельно обслуживать.

VSP2 реализует сервисные функции, например, база данных журналов, обработка передачи, доступ технического специалиста и энергонезависимое запоминающее устройство. Некоторые из этих функций зависят от данных участка эксплуатации ж. д.

6.2 Интерфейсы Ответственных подключаемых модулей

Подсистемы БПА2 и БПВ2 поддерживают расширения в форме элементов Ответственных подключаемых модулей:

Интерфейс	Описание	Примеры сценариев использования
Интерфейс систем с объектными контроллерами	Этот интерфейс обеспечивает большую функциональную гибкость при поддержке различных объектных контроллеров и объектов систем с ОК	Интерфейсные ответственные протоколы для конкретного рынка, например, немецкие объектные контроллеры БД.
Интерфейс безопасного	Подключаемый модуль на этом интерфейсе отправляет указывающие сообще-	Интерфейсные ответственные протоколы для конкретного

АРК	ния и поддерживает подключение по командам уровня безопасности к важному подключаемому модулю систем с ОК	рынка, например, итальянские системы RFI ДЦ.
Интерфейс важного подключаемого модуля ILL	Обоснование использования этого интерфейса состоит в том, что он отделяет стандартный продукт от протоколов конкретного приложения. Сообщения, обмен которыми происходит по этому интерфейсу, передаются по протоколу GNG.	ITI и ITR через ответственный подключаемый модуль Subset 098.

Эти интерфейсы позволяют проектам адаптации к рынку реализовать Ответственные приложения для конкретного рынка, чтобы они выполнялись одновременно со стандартным приложением MPC2 на одном и том же аппаратном обеспечении.

6.3 Интерфейсы не ответственных подключаемых модулей

При адаптации MPC2 к определенной ДЦ это осуществляется путем добавления подключаемых модулей в VSP2.

Аналогичным образом, VSP2 может расширяться с учетом аварийных сигналов и журнальных сообщений.

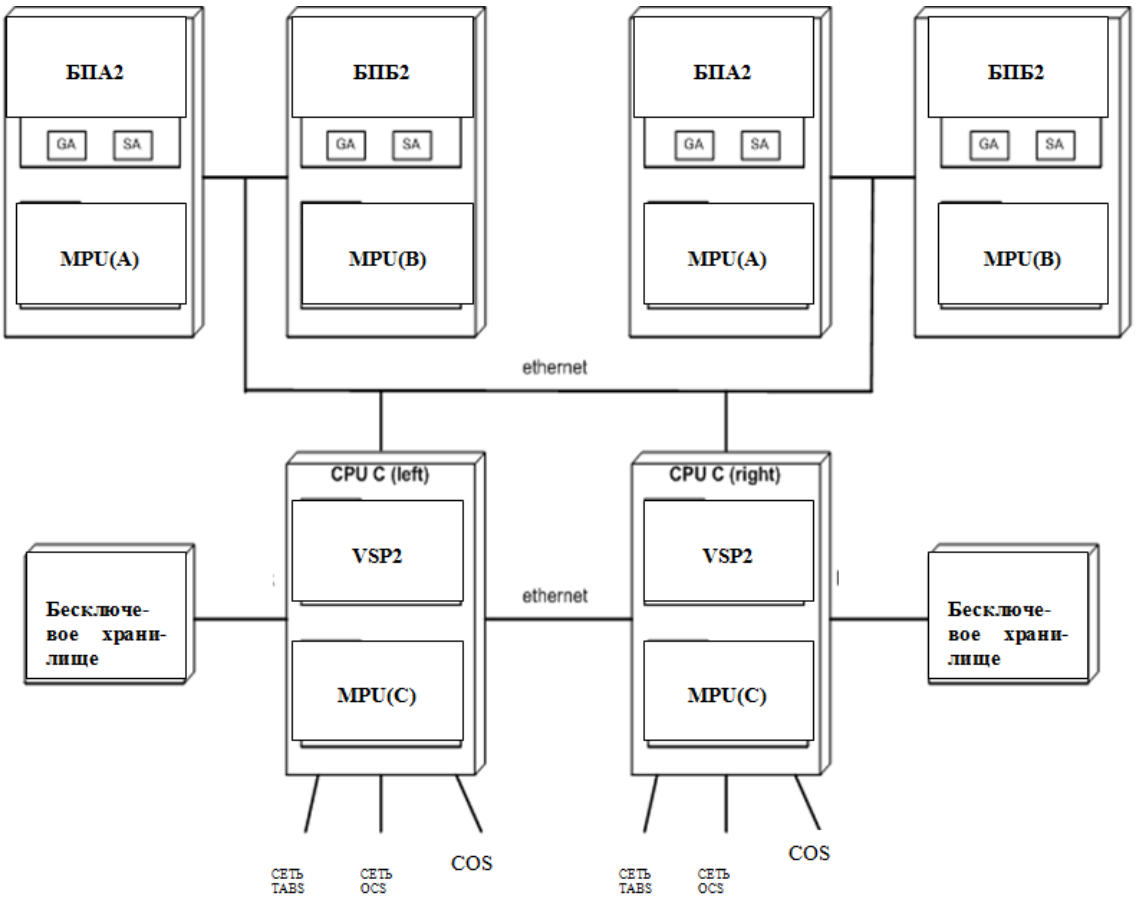

Рисунок 5 Схема развертывания MPC2

7. Функция БПА2

Выполняются следующие функции.

- Управление циклом: Цикл начинается каждые 600 мс. Длительность расчетов в каждом цикле контролируется, и при превышении предела выполняется переход в состояние ожидания.
- Неизменяющиеся данные для отдельных объектов обновляются, например, на основе команд, полученных от ДЦ.
- Неизменяющиеся данные для отдельных объектов собираются для использования в расчетах блокировки.
- Состояние, полученное из OCS, собирается для ис зования в расчетах блокировки.
- Обработка важных данных, полученных их внешних систем (например, РБЦ) через STABS2 или через важный подключаемый модуль на интерфейсе ILL.
- Обработка важных данных, полученных из подключаемого модуля на интерфейсе ILL.

- Выполняются команды, полученные от ДЦ через VSP2.
- Выполняется предварительный тест команд для предварительного теста, полученных от VSP2.
- Выполняется перекрестное сопоставление данных с данными от БПВ2. Перекрестное сопоставление происходит на разных этапах в цикле и выполняется на нескольких наборах данных.
- Перенос данных в резервный МРС2.
- Передача важных данных во внешнюю систему (например, РБЦ) через STABS2 или через важный подключаемый модуль на интерфейсе ILL.
- Передача важных данных в подключаемый модуль на интерфейсе ILL.
- Передача команд в OCS через VSP2.
- Выполнение функции взаимного наблюдения с VSP2.
- Получение данных о состоянии и отправка команд в важные подключаемые модули сортировочной станции
- Получение команд и отправка показаний в важный подключаемый модуль ДЦ.

7.1 Интерфейсы

- Интерфейс между продуктами БПА и VSP
- Интерфейс кросс-сравнения продукта БПА
- Интерфейс основной резервный продукта БПА
- Интерфейс между продуктами БПА и STABSA
- Интерфейс между продуктами БПА и безопасным плагином объектных контроллеров
- Интерфейс между продуктами БПА и безопасным плагином увязки с ДЦ
- Интерфейс между продуктами БПА и безопасным плагином увязки с ДЦ

7.2 Уровень полноты безопасности

Уровень безопасности 4 по Cenelec