Руководитель Испытательного Центра железнодорожной автоматики и телемеханики.

Наседкин Олег Андреевич

Методы обеспечения функциональной безопасности систем железнодорожной автоматики

- **Безопасность функционирования системы [устройства] железнодорожной автоматики и телемеханики:** свойство системы [устройства] железнодорожной автоматики и телемеханики обеспечивать **технологическую безопасность** и **безопасное поведение при систематических, случайных отказах аппаратных или аппаратно-программных средств и внешних воздействиях, включая ошибки операторов**.

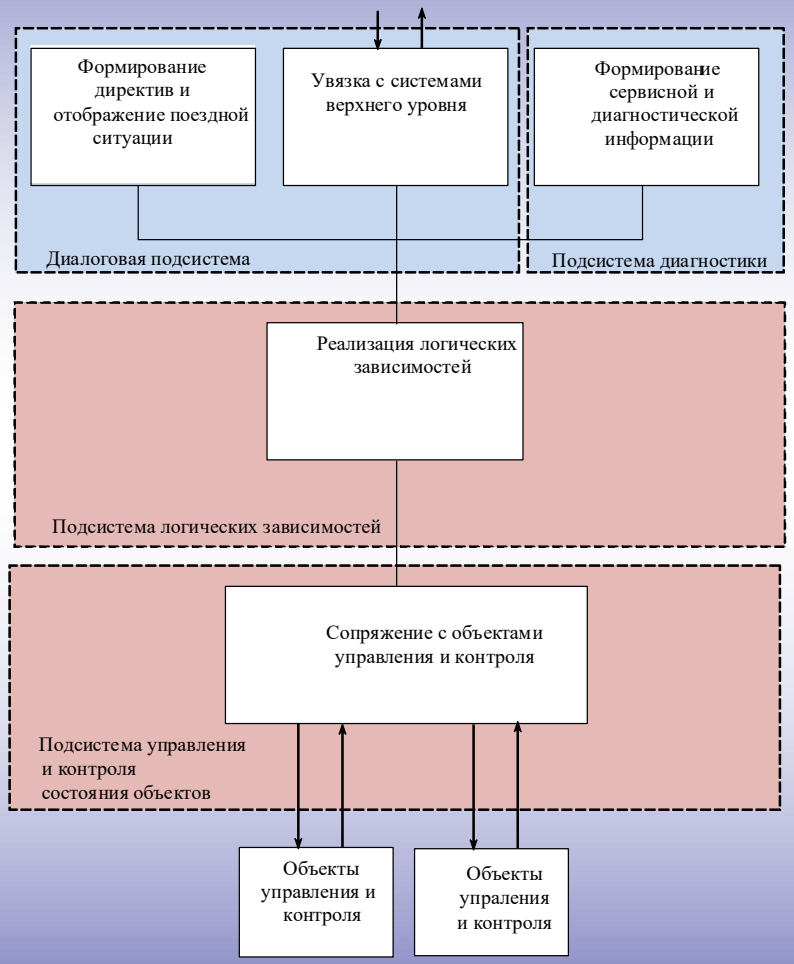
интенсивности опасных отказов основных устройств железнодорожной автоматики

- реле первого класса надежности -1,4 х 10-11;
- светофоры - 2,4 х 10-10;
- рельсовые цепи - 2,7 х 10-9;
- релейные шкафы - 2,6 х 10-9;
- электрическая централизация (на стрелку) - 7,7 х 10-9;
- автоблокировка (на сигнальную точку) - 9,2 х 10-9;
- автоматическая переездная сигнализация (на переезд) - 5,6 х 10-9.

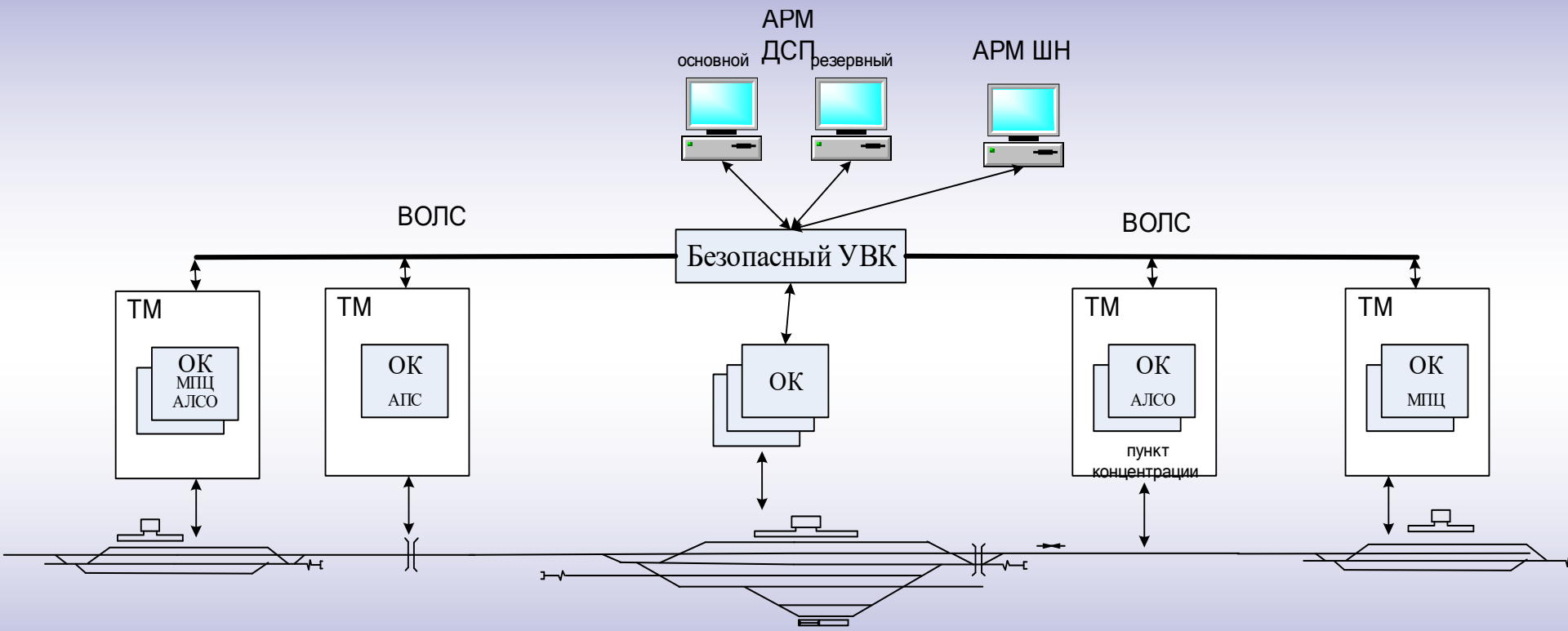
Факторы влияющие на безопасность

- отказы аппаратуры
- ошибки в исходных требованиях
- ошибки процессов разработки, изготовления и проектирования
- влияния внешней среды (электромагнитное, климатические и механические воздействия)
- ошибочные действия персонала

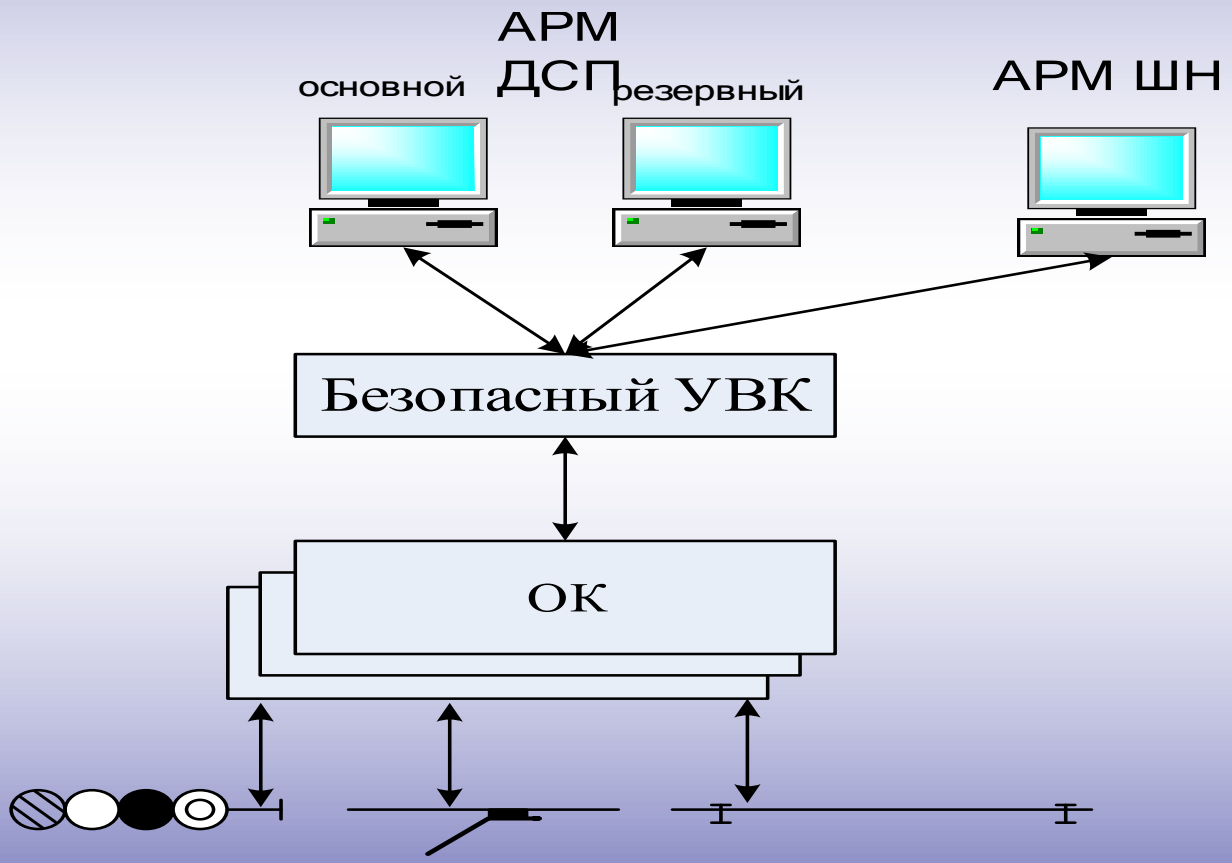
Функциональная структура системы управления



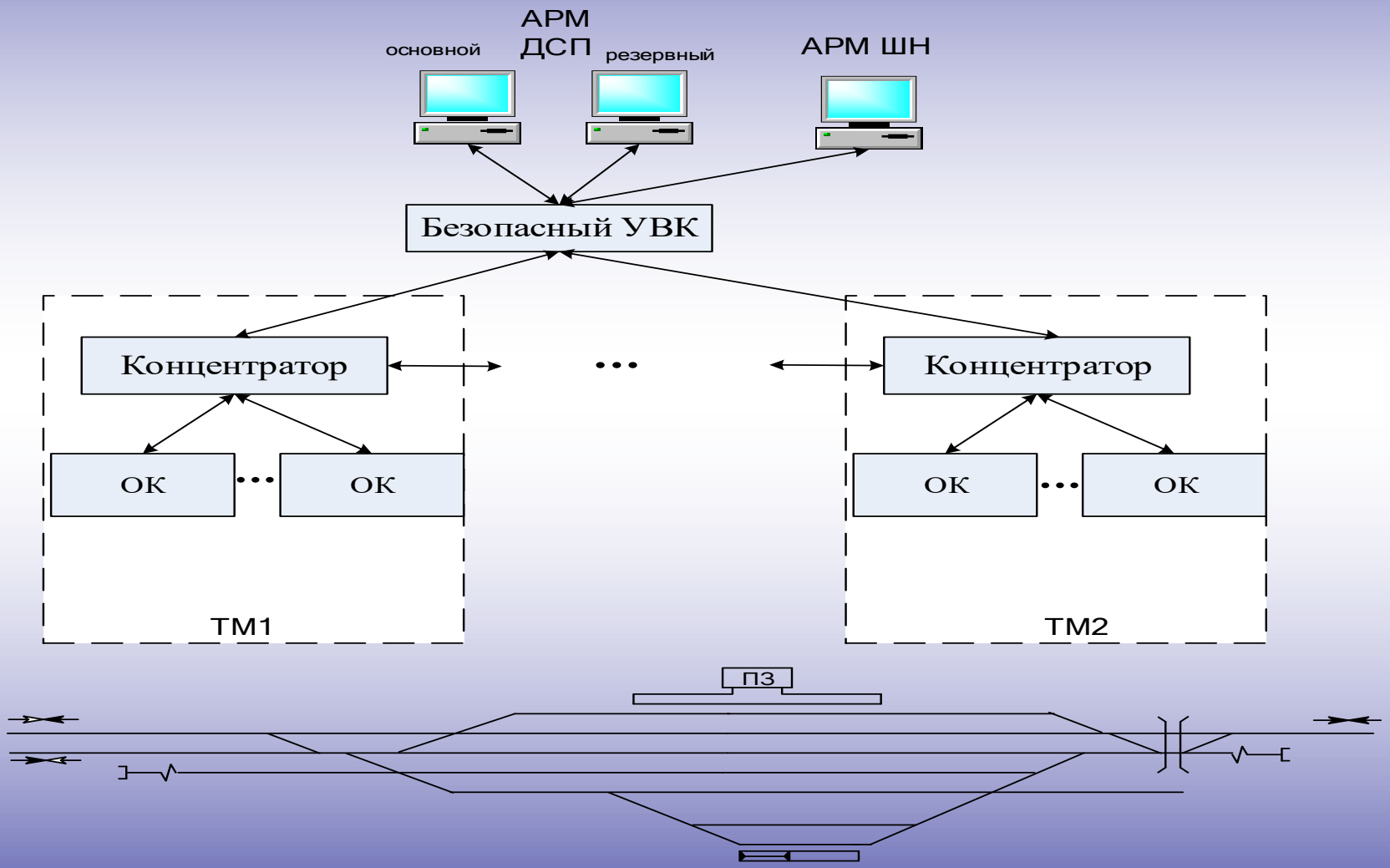
Распределённая система управления.

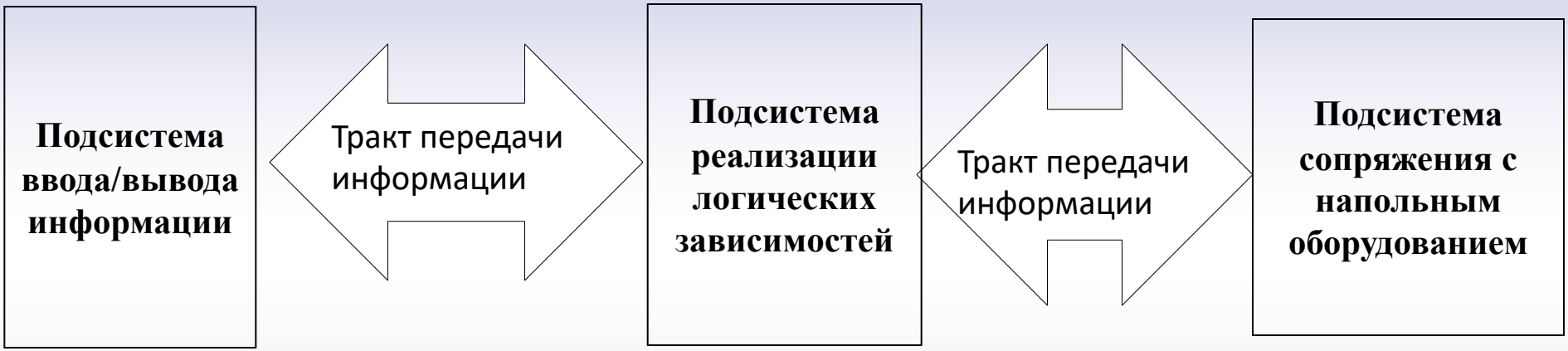


Система с централизованным размещением оборудования



Система с децентрализованным размещением оборудования



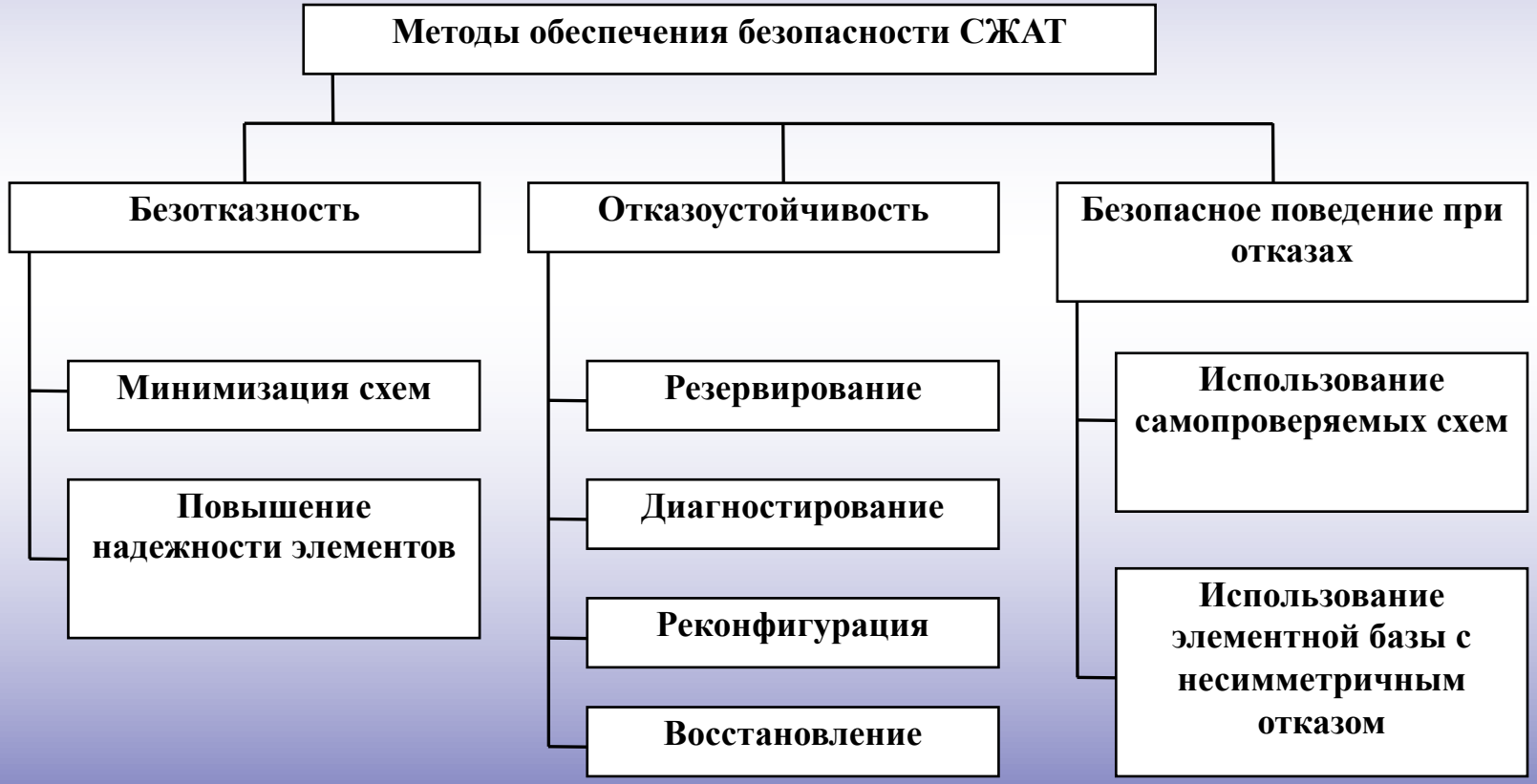

Подсистема ввода/вывода информации
Тракт передачи информации
Подсистема реализации логических зависимостей
Тракт передачи информации
Подсистема сопряжения с напольным оборудованием

Концепция безопасности микроэлектронных устройств и систем ЖАТ.

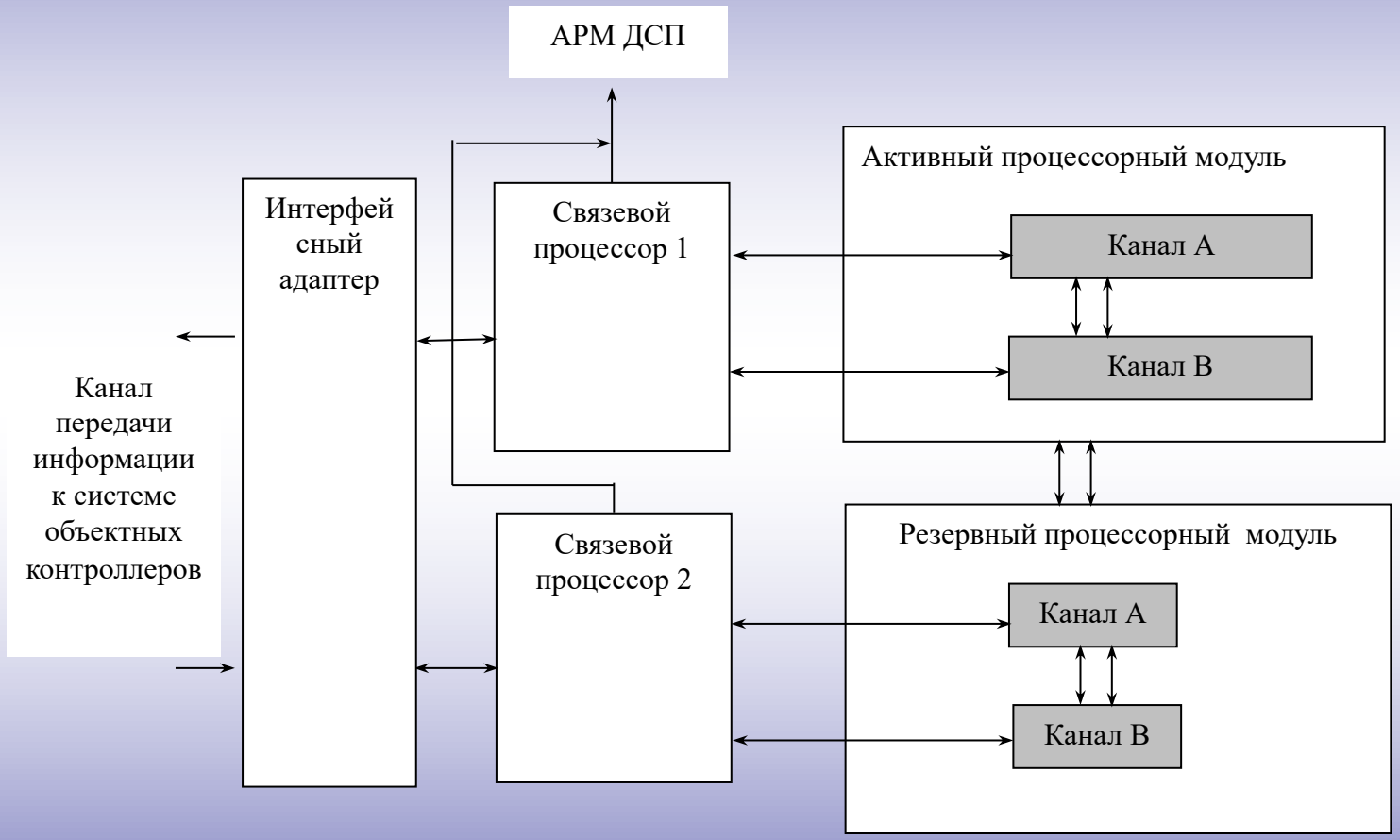
- Одиночные дефекты аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться с заданной вероятностью на рабочих и тестовых воздействиях не позднее, чем в системе возникнет второй дефект.
- Если система при возникновении отказов система исчерпала свои резервные возможности и в результате деградации и реконфигурации перестала быть отказоустойчивой, то при появлении ещё одного отказа она должна необратимо перейти в защитное (отключенное объектов управления).

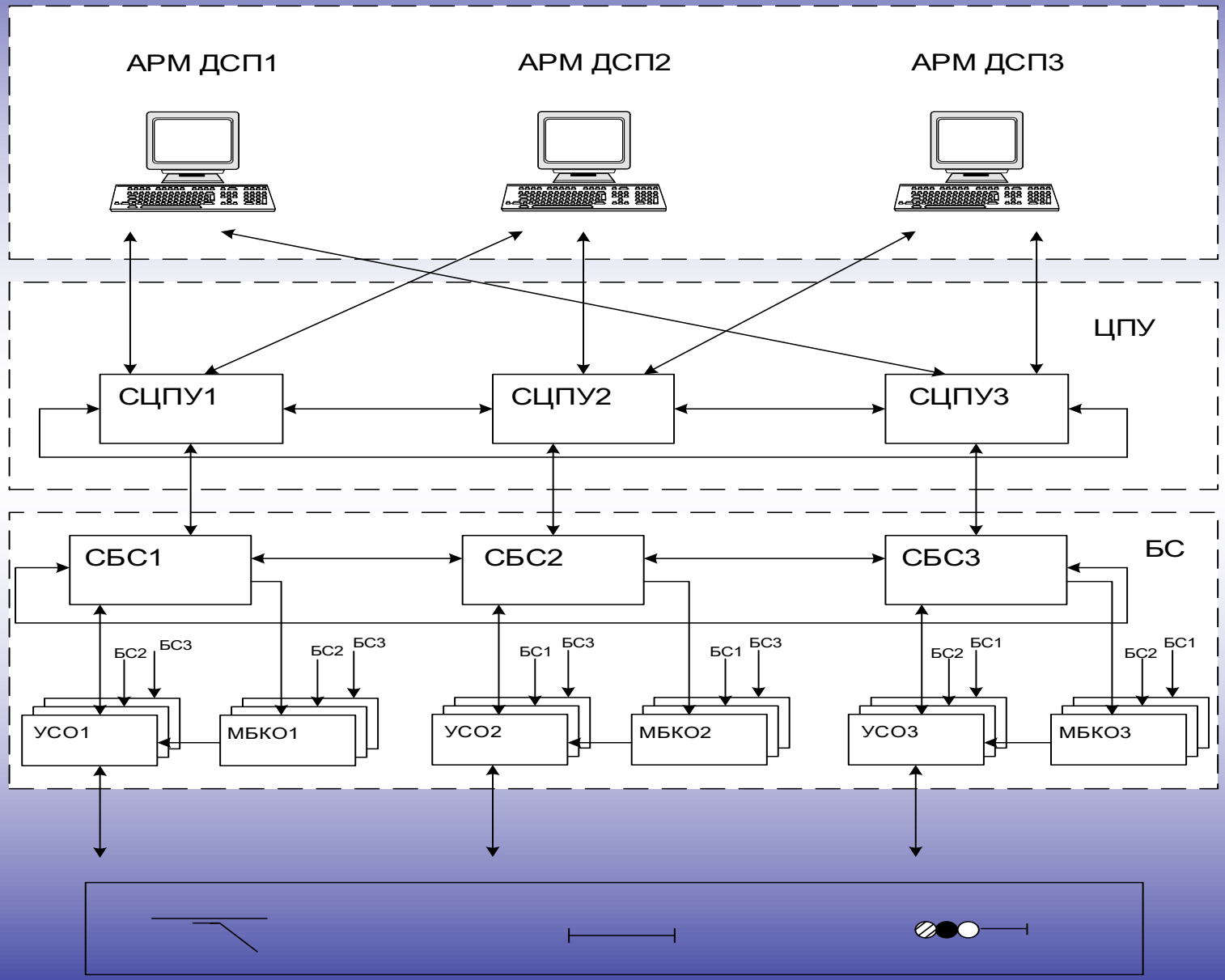
Концепция безопасности микроэлектронных устройств и систем железнодорожной автоматики

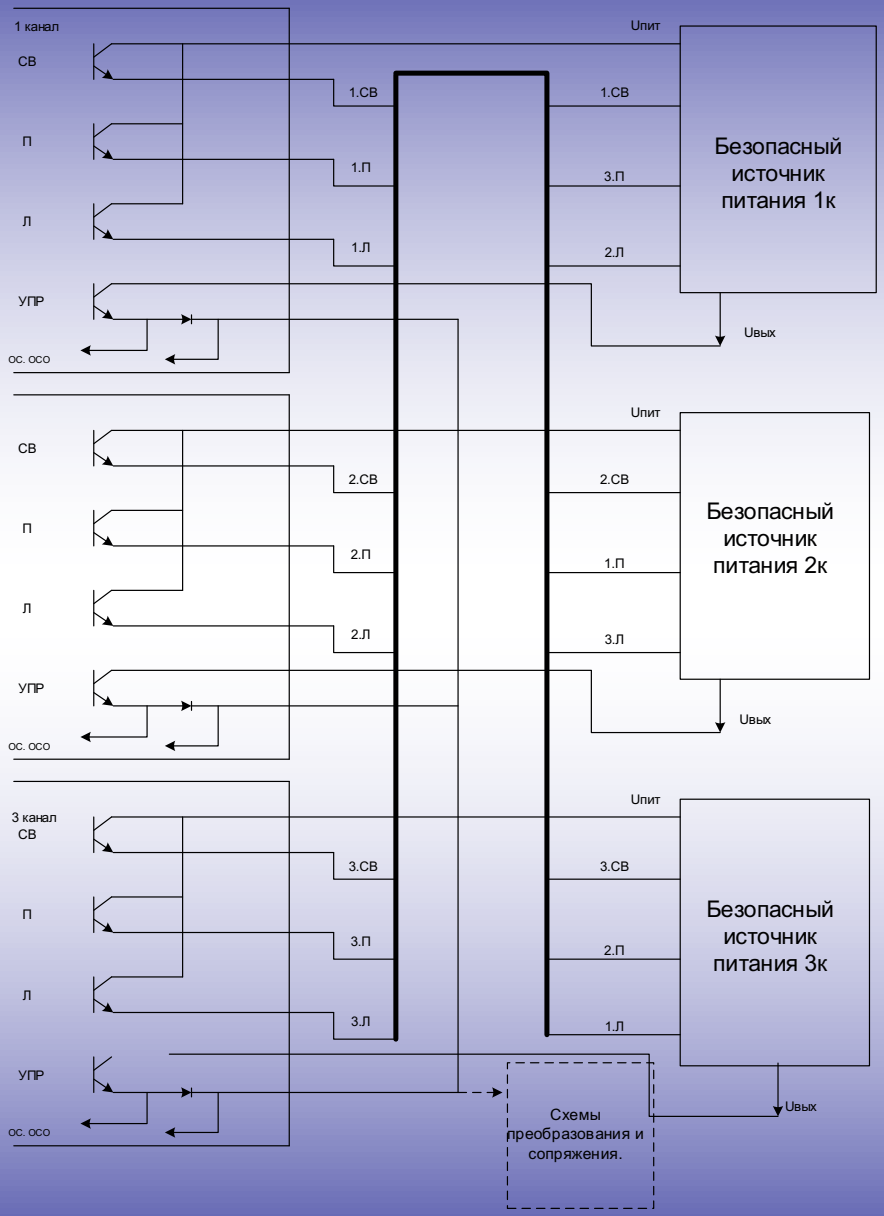
- Совокупная вероятность отказов элементов при которых система переходит в опасное состояние не должна превышать вероятности опасного отказа, заданного в требованиях на систему.


Методы обеспечения безопасности СЖАТ
Безотказность
Минимизация схем
Повышение надежности элементов
Отказоустойчивость
Резервирование
Диагностирование
Реконфигурация
Восстановление
Безопасное поведение при отказах
Использование самопроверяемых схем
Использование элементной базы с несимметричным отказом

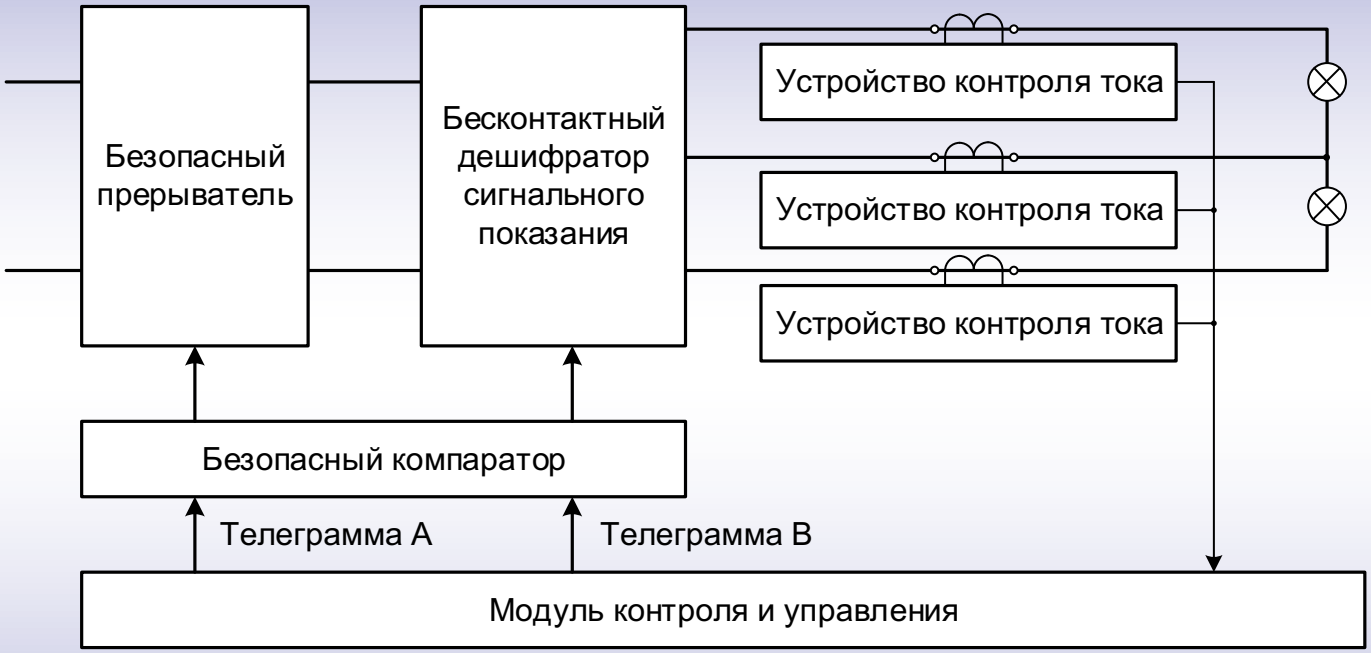
Структура технических средств

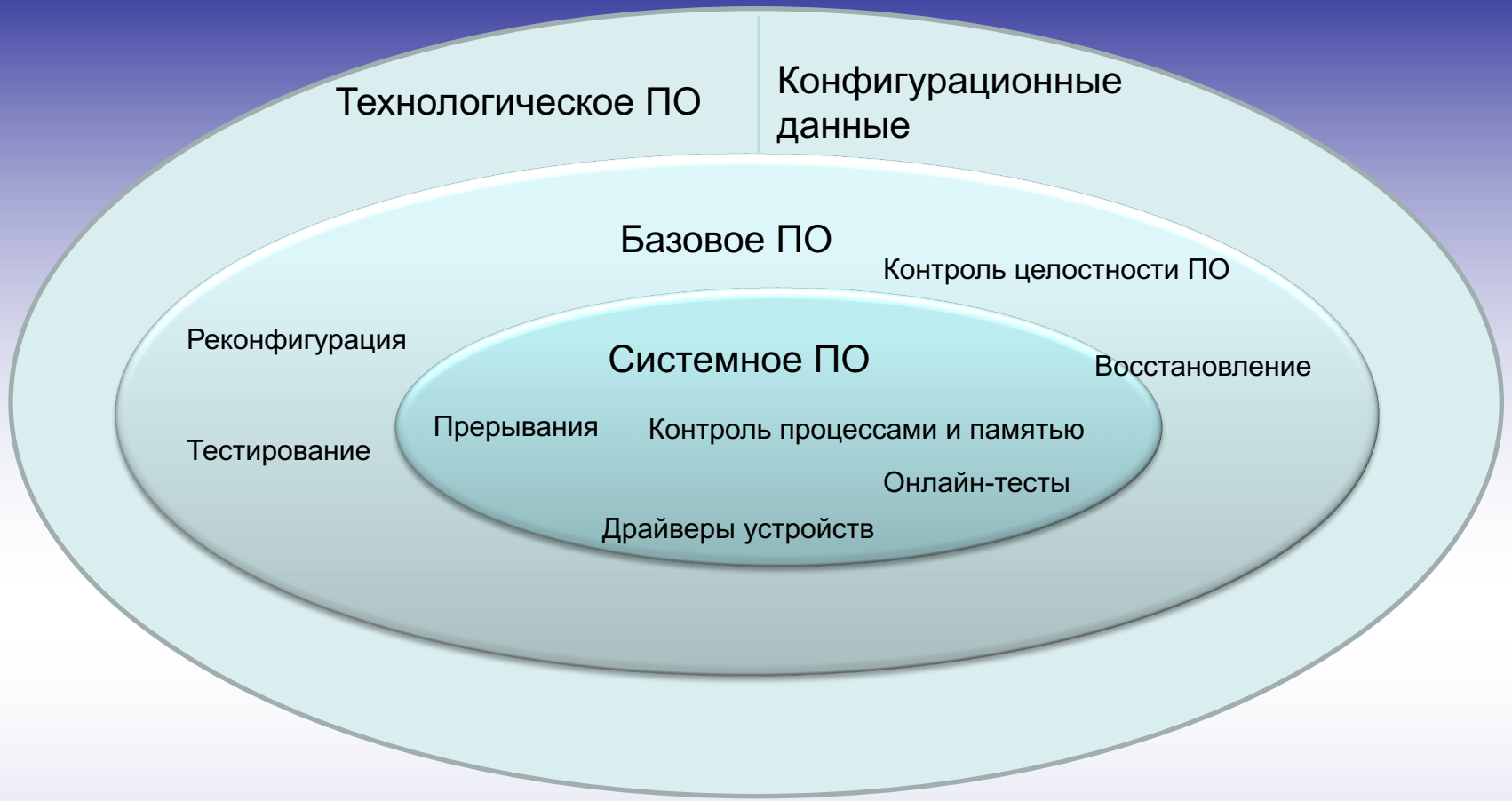



АРМ ДСП1
АРМ ДСП2
АРМ ДСП3
ЦПУ
СЦПУ1
СЦПУ2
СЦПУ3
БС
СБС1
СБС2
СБС3
БС2
БС3
БС1
БС3
БС2
БС3
БС1
БС3
БС2
БС1
БС2
БС1
УСО1
МБКО1
УСО2
МБКО2
УСО3
МБКО3


1 канал
СВ
П
Л
УПР
ос. осо
1.СВ
1.П
1.Л
Uпит
1.СВ
3.П
2.Л
Безопасный источник питания 1к
Uвых
СВ
П
Л
УПР
ос. осо
2.СВ
2.П
2.Л
Uпит
2.СВ
1.П
3.Л
Безопасный источник питания 2к
Uвых
3 канал
СВ
П
Л
УПР
ос. осо
3.СВ
3.П
3.Л
Uпит
3.СВ
2.П
1.Л
Безопасный источник питания 3к
Uвых
Схемы преобразования и сопряжения.

Модуль управления лампами светофора




Технологическое ПО
Конфигурационные данные
Базовое ПО
Контроль целостности ПО
Реконфигурация
Системное ПО
Восстановление
Прерывания
Контроль процессами и памятью
Тестирование
Онлайн-тесты
Драйверы устройств

Безопасность ПО
Реализация функций технологических алгоритмов с учетом проверки условий обеспечения безопасности движения поездов
Реализация функций управляющего вычис-лительного комплекса, определяющих его поведение в условиях возникновения отказов и сбоев технических средств

Методы обеспечения безопасности ПО
Методы обеспечения безопасности при разработке и проектировании ПО
Методы обеспечения безопасности при функционировании ПО
Методы обеспечения безопасности при сопровождении ПО
Предотвращение, обнаружение ошибок и доказательство корректности программ
Повышение устойчивости ПО к ошибкам и определение безопасного поведения при отказах и сбоях технических средств
Сохранность программ и обеспечение корректности внесения изменений

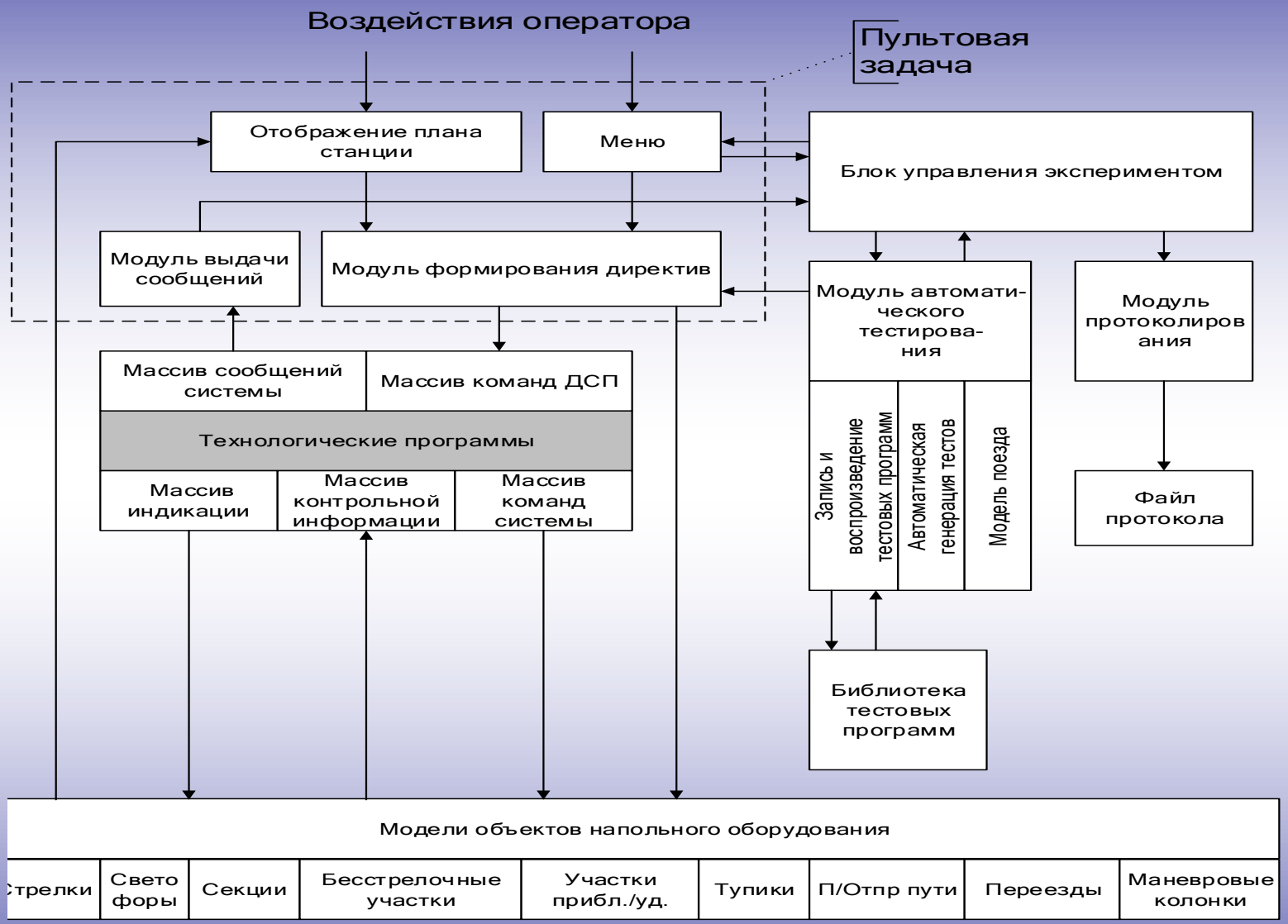
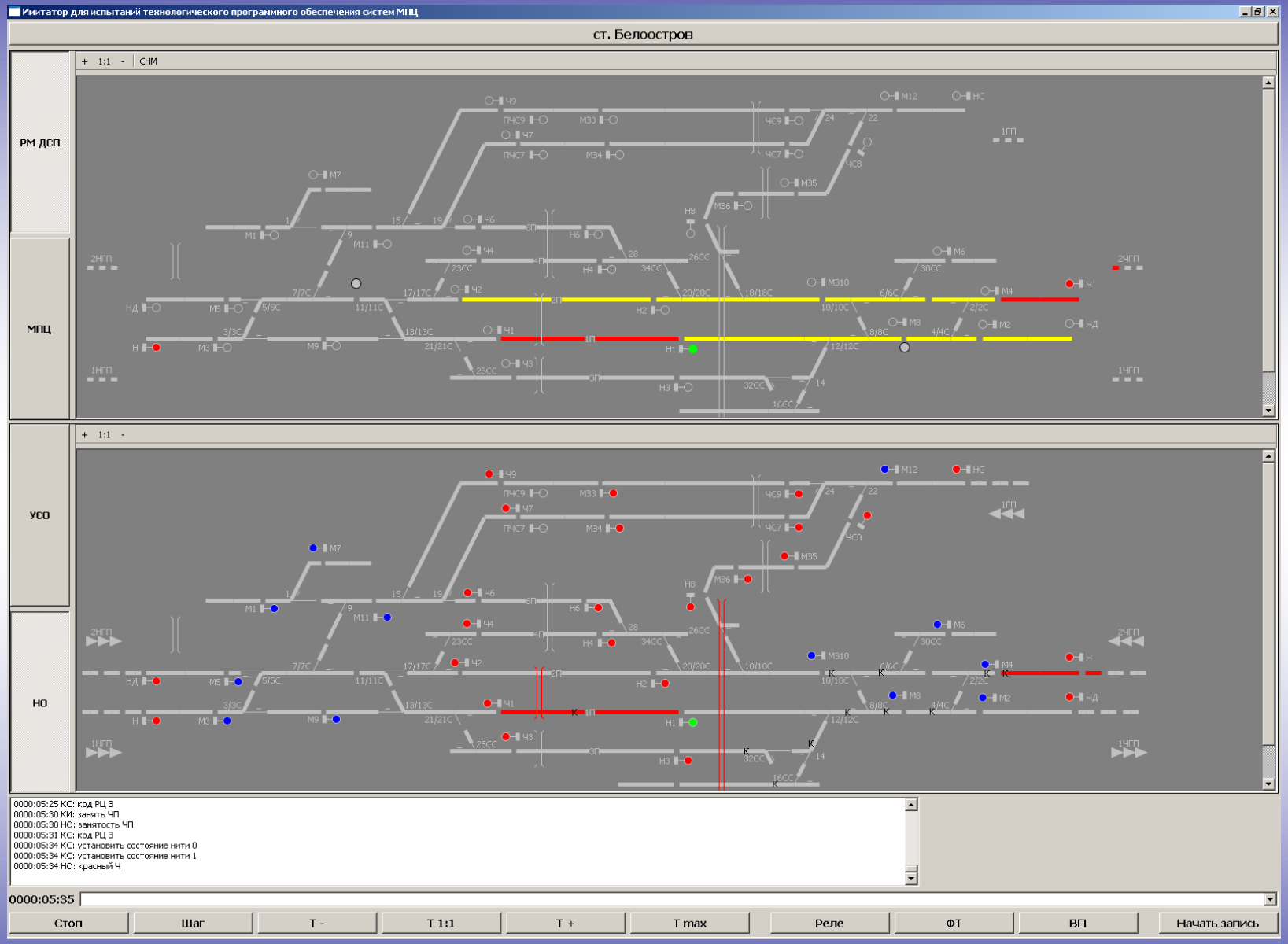
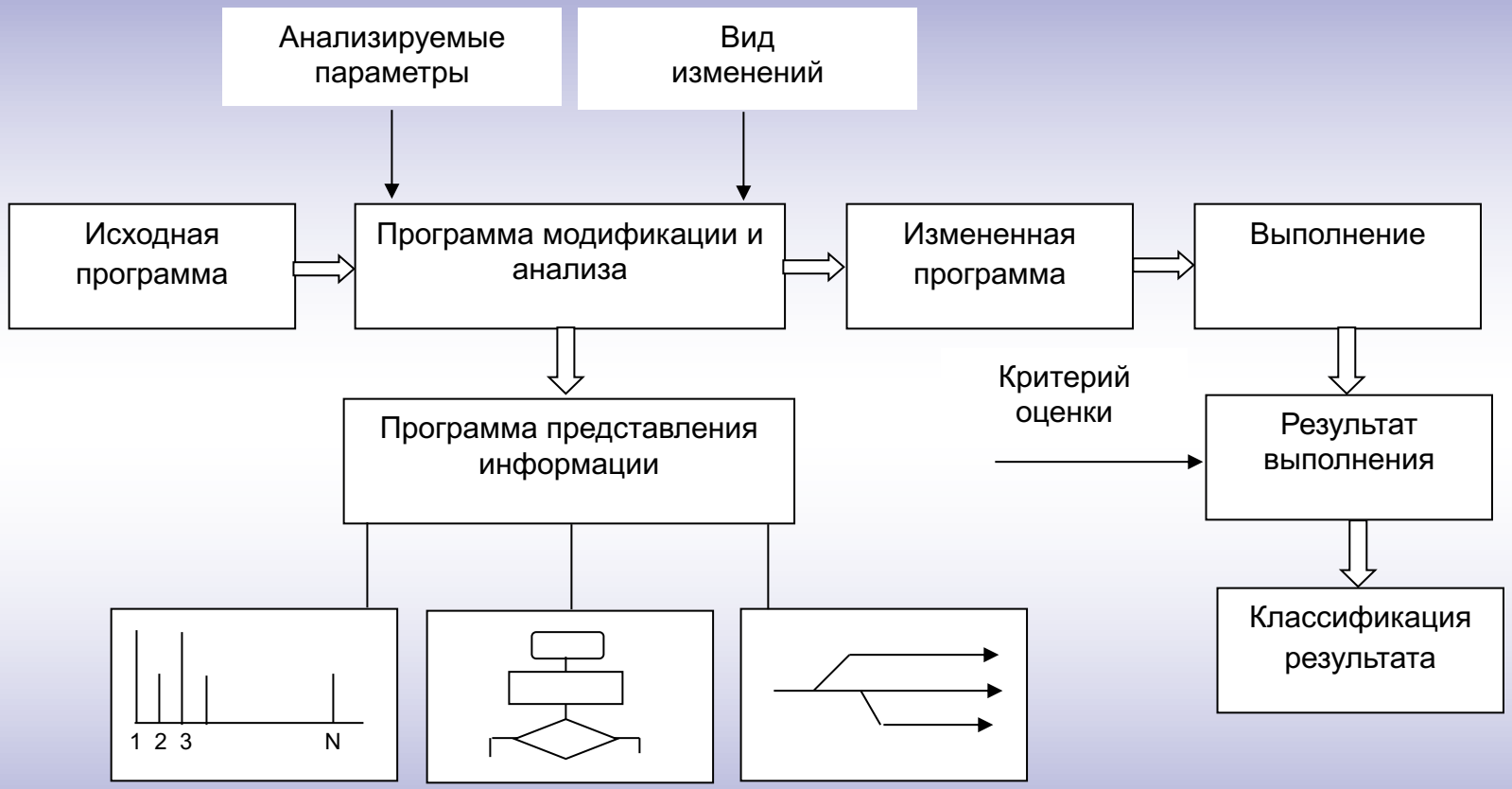


Рис 1. Структурная схема имитатора.


Имитатор для испытаний технологического программного обеспечения систем МПЦ
ст. Белоостров
РМ ДСП
МПЦ
УСО
НО
+ 1:1 - СНМ
+ 1:1 -
0000:05:25 КС: код РЦ 3
0000:05:30 КИ: занять ЧП
0000:05:30 НО: занятость ЧП
0000:05:31 КС: код РЦ 3
0000:05:34 КС: установить состояние нити 0
0000:05:34 КС: установить состояние нити 1
0000:05:34 НО: красный Ч
0000:05:35
Стоп
Шаг
Т -
Т 1:1
Т +
Т max
Реле
ФТ
ВП
Начать запись



Структурная схема средств модификации и анализа ПО

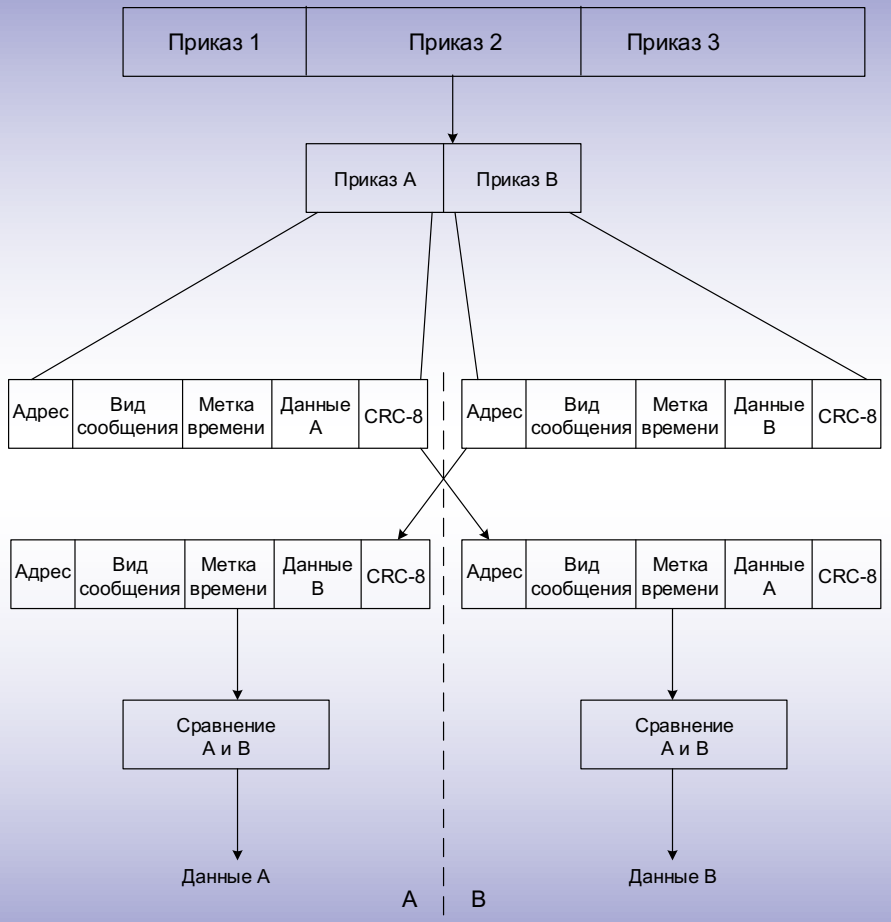
Причины опасных ситуаций при передачи данных

- - ошибки в данных (ошибки идентификации передатчика, ошибки типа данных, ошибки значений данных);
- - ошибки, связанные со временем (слишком большая задержка данных, ошибка в последовательности).

Основные задачи методов обеспечения безопасности при передачи данных.

- обнаружение ошибки идентификации передатчика.
- обнаружение ошибки в типе данных.
- обнаружение ошибки в значениях данных.
- обнаружение данных, с не установленными временными параметрами или не полученных вовремя.
- обнаружение потери связи по истечении заранее заданного допустимого промежутка времени.
- подтверждение функциональной независимости механизмов обеспечения безопасности данных

Структура телеграммы



Спасибо за внимание.