Локальная сеть цифровой подстанции с элементами «secure by design»

Максим Никандров
к.т.н., ООО «Интеллектуальные Сети»
Михаил Селезнев
ПАО «ФСК ЕЭС»

1. **Сегментирование ЛВС – с помощью программных или физических межсетевых экранов.**

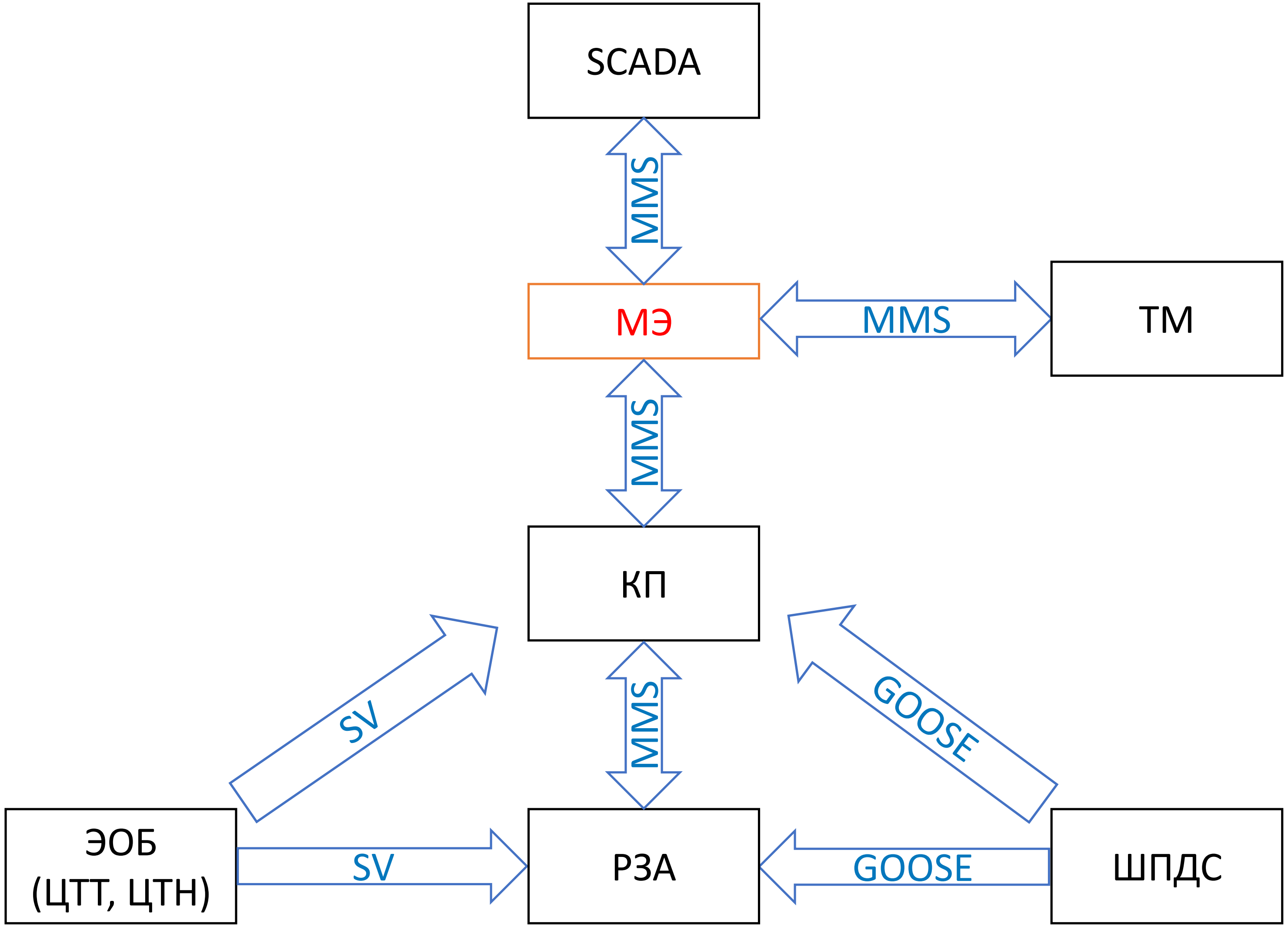
2. **Организация демилитаризованной зоны – для обеспечения информационного обмена с вышестоящими уровнями управления.**

3. **Система обнаружения вторжений – для контроля трафика в ключевых точках ЛВС.**

4. **Антивирусное обеспечение – для безопасности данных на серверах и АРМ АСУ ТП.**

5. **Центр управления ИБ (сервер ИБ) – для удаленного централизованного управления защитой.**

Сегментирование ЛВС



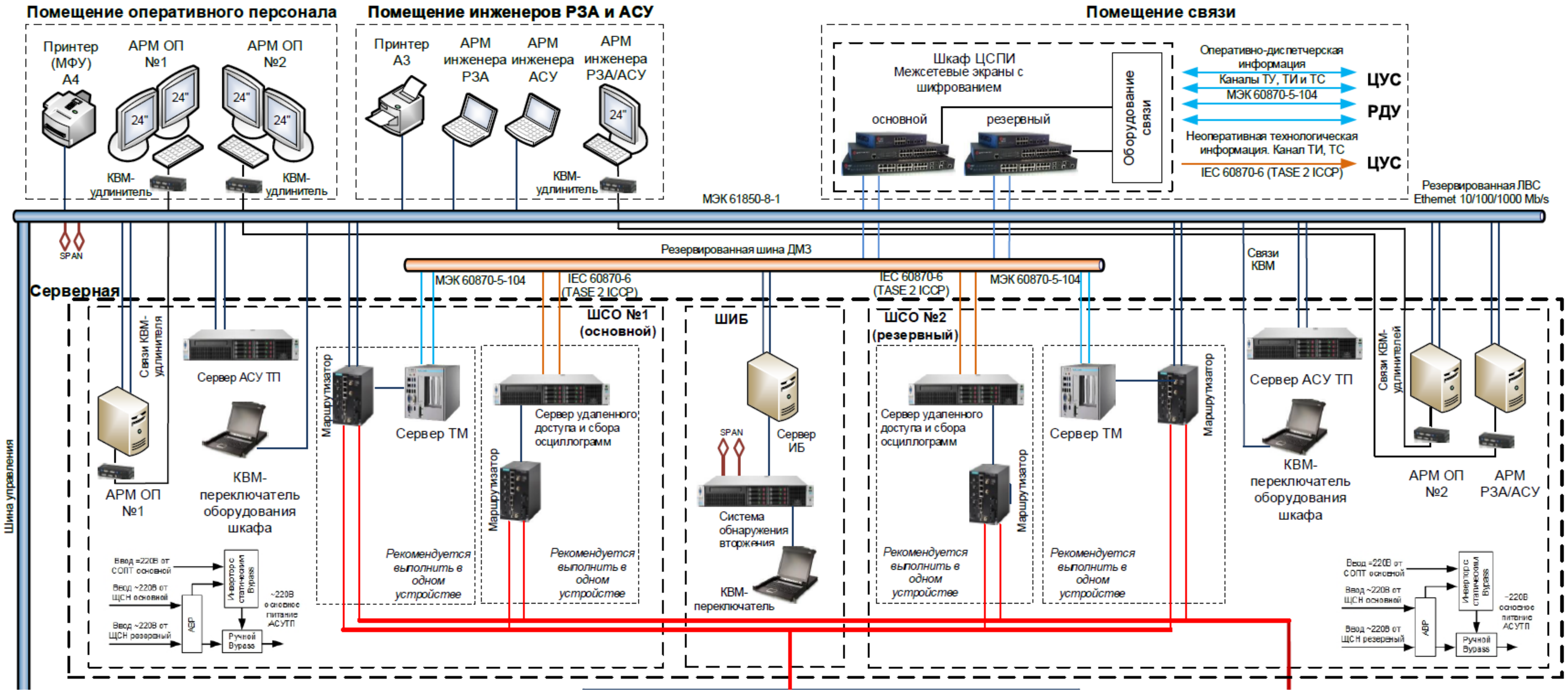
Управляемая деградация контура управления:

- потеря связи с удаленным ДП -> управление со скады;
- потеря связи со скадой -> управление с КП;
- потеря связи с КП -> управление с терминала РЗА.

Проект СТО «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС»

Предложение по выполнению требований в части ИБ

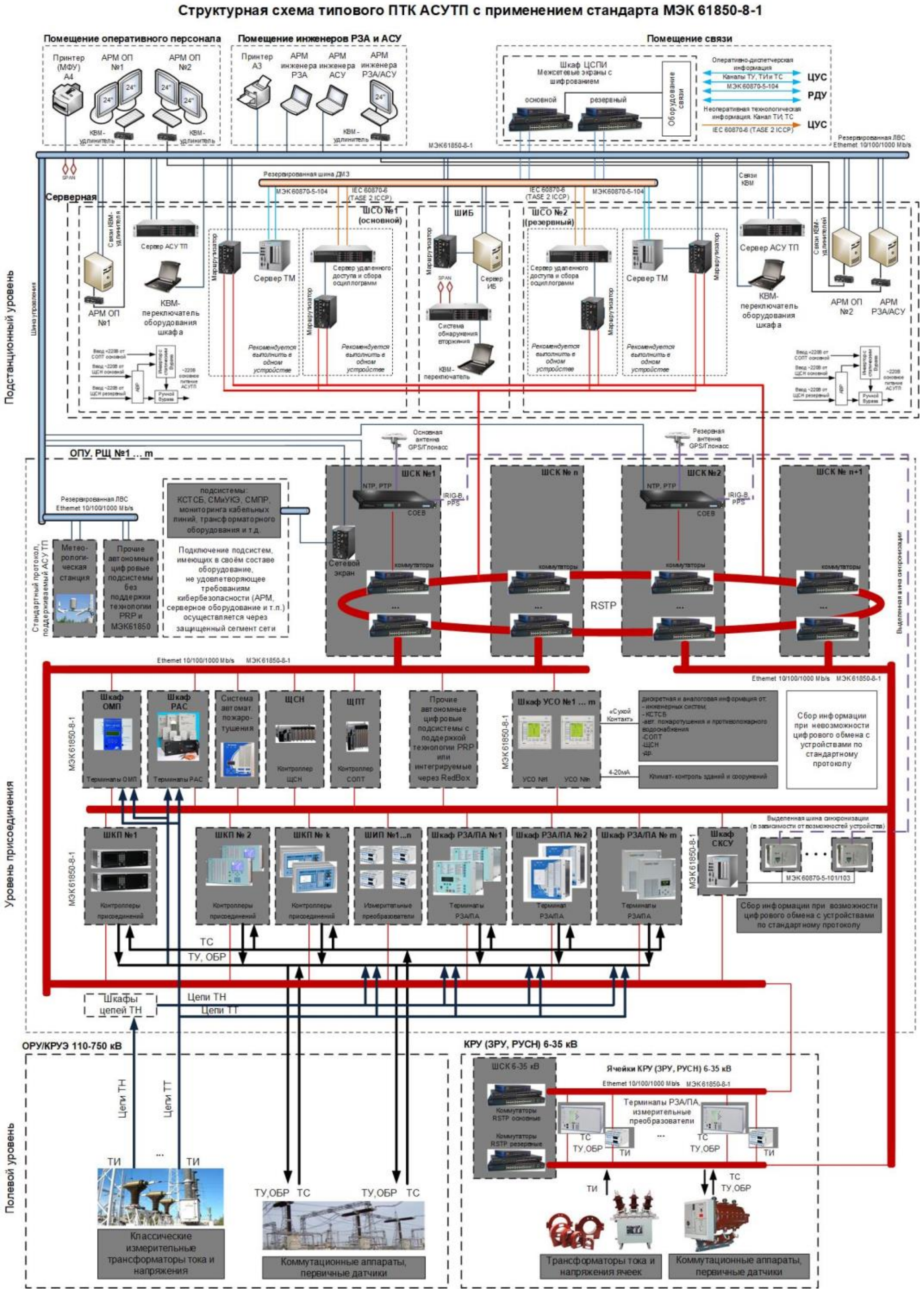
Организация ДМЗ, установка СОВ и сервера ИБ



Помещение оперативного персонала
Принтер (МФУ) А4
АРМ ОП №1
АРМ ОП №2
24"
КВМ-удлинитель
Помещение инженеров РЗА и АСУ
Принтер А3
АРМ инженера РЗА
АРМ инженера АСУ
АРМ инженера РЗА/АСУ
Помещение связи
Шкаф ЦСПИ
Межсетевые экраны с шифрованием
основной
резервный
Оборудование связи
Оперативно-диспетчерская информация
Каналы ТУ, ТИ и ТС
МЭК 60870-5-104
ЦУС
РДУ
Неоперативная технологическая информация. Канал ТИ, ТС
IEC 60870-6 (TASE 2 ICCP)
ЦУС
МЭК 61850-8-1
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
SPAN
Резервированная шина ДМЗ
МЭК 60870-5-104
IEC 60870-6 (TASE 2 ICCP)
IEC 60870-6 (TASE 2 ICCP)
МЭК 60870-5-104
Связи КВМ
Серверная
Шина управления
Связи КВМ-удлинителя
Сервер АСУ ТП
АРМ ОП №1
КВМ-переключатель оборудования шкафа
Маршрутизатор
Сервер ТМ
ШСО №1 (основной)
Сервер удаленного доступа и сбора осциллограмм
Маршрутизатор
Рекомендуется выполнить в одном устройстве
Рекомендуется выполнить в одном устройстве
ШИБ
Сервер ИБ
SPAN
Система обнаружения вторжения
КВМ-переключатель
ШСО №2 (резервный)
Сервер удаленного доступа и сбора осциллограмм
Маршрутизатор
Сервер ТМ
Маршрутизатор
Рекомендуется выполнить в одном устройстве
Рекомендуется выполнить в одном устройстве
Сервер АСУ ТП
КВМ-переключатель оборудования шкафа
Связи КВМ-удлинителей
АРМ ОП №2
АРМ РЗА/АСУ
Ввод =220В от СОПТ основной
Ввод ~220В от ЩСН основной
Ввод ~220В от ЩСН резервный
АВР
Инвертор с статическим Bypass
Ручной Bypass
~220В основное питание АСУТП
Ввод =220В от СОПТ основной
Ввод ~220В от ЩСН основной
Ввод ~220В от ЩСН резереный
АВР
Инвертор с статическим Bypass
Ручной Bypass
~220В основное питание АСУТП

Проект СТО «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС»

I архитектура


Структурная схема типового ПТК АСУТП с применением стандарта МЭК 61850-8-1

Помещение оперативного персонала
Принтер (МФУ) А4
АРМ ОП №1
АРМ ОП №2
24"
КВМ-удлинитель
Помещение инженеров РЗА и АСУ
Принтер А3
АРМ инженера РЗА
АРМ инженера АСУ
АРМ инженера РЗА/АСУ
Помещение связи
Шкаф ЦСПИ
Межсетевые экраны с шифрованием
основной
резервный
Оборудование связи
Оперативно-диспетчерская информация
Каналы ТУ, ТИ и ТС
МЭК 60870-5-104
ЦУС
РДУ
Неоперативная технологическая информация. Канал ТИ, ТС
IEC 60870-6 (TASE 2 ICCP)
ЦУС
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
МЭК61850-8-1
SPAN
Резервированная шина ДМЗ
МЭК 60870-5-104
IEC 60870-6 (TASE 2 ICCP)
Серверная
Связи КВМ-удлинителя
Сервер АСУ ТП
КВМ-переключатель оборудования шкафа
ШСО №1 (основной)
Маршрутизатор
Сервер ТМ
Сервер удаленного доступа и сбора осциллограмм
Рекомендуется выполнить в одном устройстве
ШИБ
Сервер ИБ
Система обнаружения вторжения
КВМ-переключатель
ШСО №2 (резервный)
Связи КВМ
Связи КВМ-удлинителей
АРМ ОП №2
АРМ РЗА/АСУ
Ввод ~220В от СОПТ основной
Ввод ~220В от ЩСН основной
Ввод ~220В от ЩСН резервный
АВР
Инвертор с статическим bypass
Ручной bypass
~220В основное питание АСУТП
Подстанционный уровень
Шина управления
Основная антенна GPS/Глонасс
Резервная антенна GPS/Глонасс
ОПУ, РЩ №1 … m
ШСК №1
ШСК № n
ШСК №2
ШСК № n+1
NTP, PTP
IRIG-B, PPS
СОЕВ
коммутаторы
RSTP
Сетевой экран
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
подсистемы: КСТСБ, СМиУКЭ, СМПР, мониторинга кабельных линий, трансформаторного оборудования и т.д.
Подключение подсистем, имеющих в своём составе оборудование, не удовлетворяющее требованиям кибербезопасности (АРМ, серверное оборудование и т.п.) осуществляется через защищенный сегмент сети
Стандартный протокол, поддерживаемый АСУ ТП
Метеорологическая станция
Прочие автономные цифровые подсистемы без поддержки технологии PRP и МЭК61850
Выделенная шина синхронизации
Ethernet 10/100/1000 Mb/s МЭК61850-8-1
Шкаф ОМП
Терминалы ОМП
Шкаф РАС
Терминалы РАС
Система автомат. пожаротушения
ЩСН
Контроллер ЩСН
ЩПТ
Контроллер СОПТ
Прочие автономные цифровые подсистемы с поддержкой технологии PRP или интегрируемые через RedBox
Шкаф УСО №1 … m
УСО №1
УСО №n
«Сухой Контакт»
дискретная и аналоговая информация от: - инженерных систем; - КСТСБ -авт. пожаротушения и противопожарного водоснабжения -СОПТ -ЩСН -др.
4-20мА
Климат-контроль зданий и сооружений
Сбор информации при невозможности цифрового обмена с устройствами по стандартному протоколу
МЭК61850-8-1
ШКП №1
ШКП № 2
ШКП № k
Контроллеры присоединений
ШИП №1…n
Измерительные преобразователи
Шкаф РЗА/ПА №1
Шкаф РЗА/ПА №2
Шкаф РЗА/ПА № m
Терминалы РЗА/ПА
Шкаф СКСУ
Выделенная шина синхронизации (в зависимости от возможностей устройства)
МЭК 60870-5-101/103
Сбор информации при возможности цифрового обмена с устройствами по стандартному протоколу
ТС
ТУ, ОБР
Шкафы цепей ТН
Цепи ТН
Цепи ТТ
Уровень присоединения
ОРУ/КРУЭ 110-750 кВ
ТИ
Классические измерительные трансформаторы тока и напряжения
ТУ,ОБР
Коммутационные аппараты, первичные датчики
КРУ (ЗРУ, РУСН) 6-35 кВ
ШСК 6-35 кВ
Коммутаторы RSTP основные
Коммутаторы RSTP резервные
Ячейки КРУ (ЗРУ, РУСН) 6-35 кВ
Терминалы РЗА/ПА, измерительные преобразователи
Трансформаторы тока и напряжения ячеек
Полевой уровень

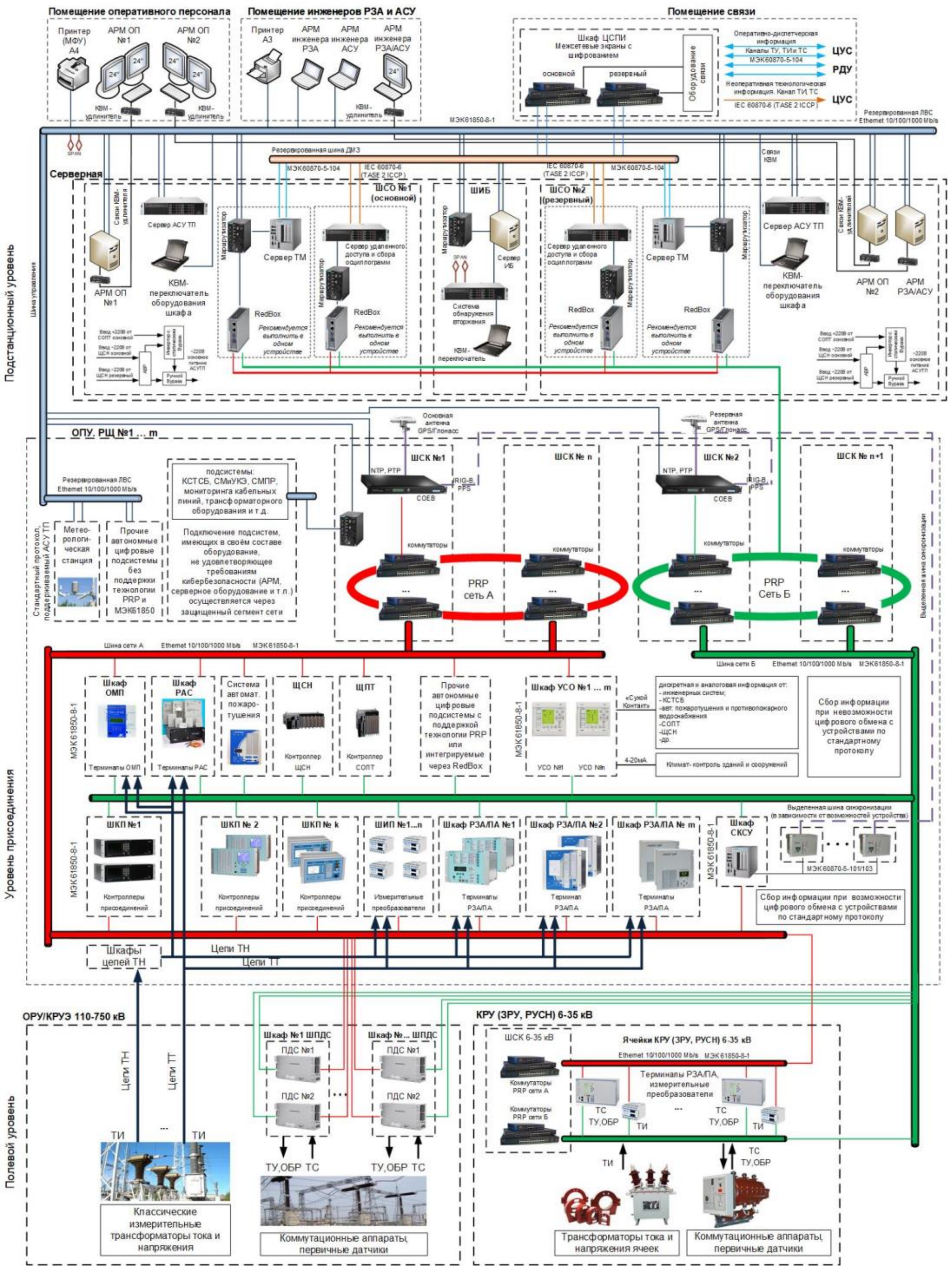
Особенности:

- для подстанций с недавно модернизированной АСУ ТП;
- применение протоколов RSTP и PRP;
- без использования протоколов GOOSE и SV;
- без ШПДС и ШПАС;
- изменения только на подстанционном уровне в части ИБ.

Проект СТО «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС»

II архитектура

Структурная схема типового ПТК АСУТП с применением стандарта МЭК 61850-8-1



Помещение оперативного персонала
Принтер (МФУ) А4
АРМ ОП №1
АРМ ОП №2
24"
КВМ-удлинитель
Помещение инженеров РЗА и АСУ
Принтер А3
АРМ инженера РЗА
АРМ инженера АСУ
АРМ инженера РЗА/АСУ
Помещение связи
Шкаф ЦСПИ
Межсетевые экраны с шифрованием
основной
резервный
Оборудование связи
Оперативно-диспетчерская информация
Каналы ТУ, ТИ и ТС
МЭК60870-5-104
ЦУС
РДУ
Неоперативная технологическая информация. Канал ТИ, ТС
IEC 60870-6 (TASE 2 ICCP)
ЦУС
МЭК61850-8-1
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
SPAN
Резервированная шина ДМЗ
МЭК60870-5-104
IEC 60870-6 (TASE 2 ICCP)
Связи КВМ
Серверная
Шина управления
Связи КВМ-удлинителя
Сервер АСУ ТП
АРМ ОП №1
КВМ-переключатель оборудования шкафа
ШСО №1 (основной)
Маршрутизатор
Сервер ТМ
Сервер удаленного доступа и сбора осциллограмм
RedBox
Рекомендуется выполнить в одном устройстве
ШИБ
Сервер ИБ
Система обнаружения вторжения
КВМ-переключатель
ШСО №2 (резервный)
Связи КВМ-удлинителей
АРМ ОП №2
АРМ РЗА/АСУ
Ввод ~220В от СОПТ основной
Ввод ~220В от ЩСН основной
Ввод ~220В от ЩСН резервный
АВР
Инвертор с статическим байпасом
Ручной Байпас
~220В основное питание АСУТП
Подстанционный уровень
ОПУ. РЩ №1 … m
Основная антенна GPS/Глонасс
Резервная антенна GPS/Глонасс
ШСК №1
ШСК № n
ШСК №2
ШСК № n+1
NTP, PTP
IRIG-B, PPS
СОЕВ
коммутаторы
PRP сеть А
PRP Сеть Б
Выделенная шина синхронизации
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
Стандартный протокол, поддерживаемый АСУ ТП
Метео-рологи-ческая станция
Прочие автономные цифровые подсистемы без поддержки технологии PRP и МЭК61850
подсистемы: КСТСБ, СМиУКЭ, СМПР, мониторинга кабельных линий, трансформаторного оборудования и т.д.
Подключение подсистем, имеющих в своём составе оборудование, не удовлетворяющее требованиям кибербезопасности (АРМ, серверное оборудование и т.п.) осуществляется через защищенный сегмент сети
Шина сети А
Ethernet 10/100/1000 Mb/s
МЭК61850-8-1
Шина сети Б
Ethernet 10/100/1000 Mb/s
МЭК61850-8-1
Уровень присоединения
МЭК61850-8-1
Шкаф ОМП
Терминалы ОМП
Шкаф РАС
Терминалы РАС
Система автомат. пожаро-тушения
ЩСН
Контроллер ЩСН
ЩПТ
Контроллер СОПТ
Прочие автономные цифровые подсистемы с поддержкой технологии PRP или интегрируемые через RedBox
Шкаф УСО №1 … m
УСО №1
УСО №n
«Сухой Контакт»
дискретная и аналоговая информация от:
- инженерных систем;
- КСТСБ
- авт. пожаротушения и противопожарного водоснабжения
- СОПТ
- ЩСН
- др.
4-20мА
Климат-контроль зданий и сооружений
Сбор информации при невозможности цифрового обмена с устройствами по стандартному протоколу
ШКП №1
ШКП № 2
ШКП № k
Контроллеры присоединений
ШИП №1...n
Измерительные преобразователи
Шкаф РЗА/ПА №1
Шкаф РЗА/ПА №2
Шкаф РЗА/ПА № m
Терминалы РЗА/ПА
Терминал РЗА/ПА
Шкаф СКСУ
Выделенная шина синхронизации (в зависимости от возможностей устройства)
МЭК60870-5-101/103
Сбор информации при возможности цифрового обмена с устройствами по стандартному протоколу
Шкафы цепей ТН
Цепи ТН
Цепи ТТ
ОРУ/КРУЭ 110-750 кВ
Полевой уровень
Цепи ТН
Цепи ТТ
ТИ
ТИ
Классические измерительные трансформаторы тока и напряжения
Шкаф №1 ШПДС
Шкаф №... ШПДС
ПДС №1
ПДС №2
ТУ,ОБР ТС
Коммутационные аппараты, первичные датчики
КРУ (ЗРУ, РУСН) 6-35 кВ
ШСК 6-35 кВ
Коммутаторы PRP сети А
Коммутаторы PRP сети Б
Ячейки КРУ (ЗРУ, РУСН) 6-35 кВ
Ethernet 10/100/1000 Mb/s МЭК61850-8-1
Терминалы РЗА/ПА, измерительные преобразователи
ТС
ТУ,ОБР
ТИ
ТИ
ТС ТУ,ОБР
Трансформаторы тока и напряжения ячеек
Коммутационные аппараты, первичные датчики

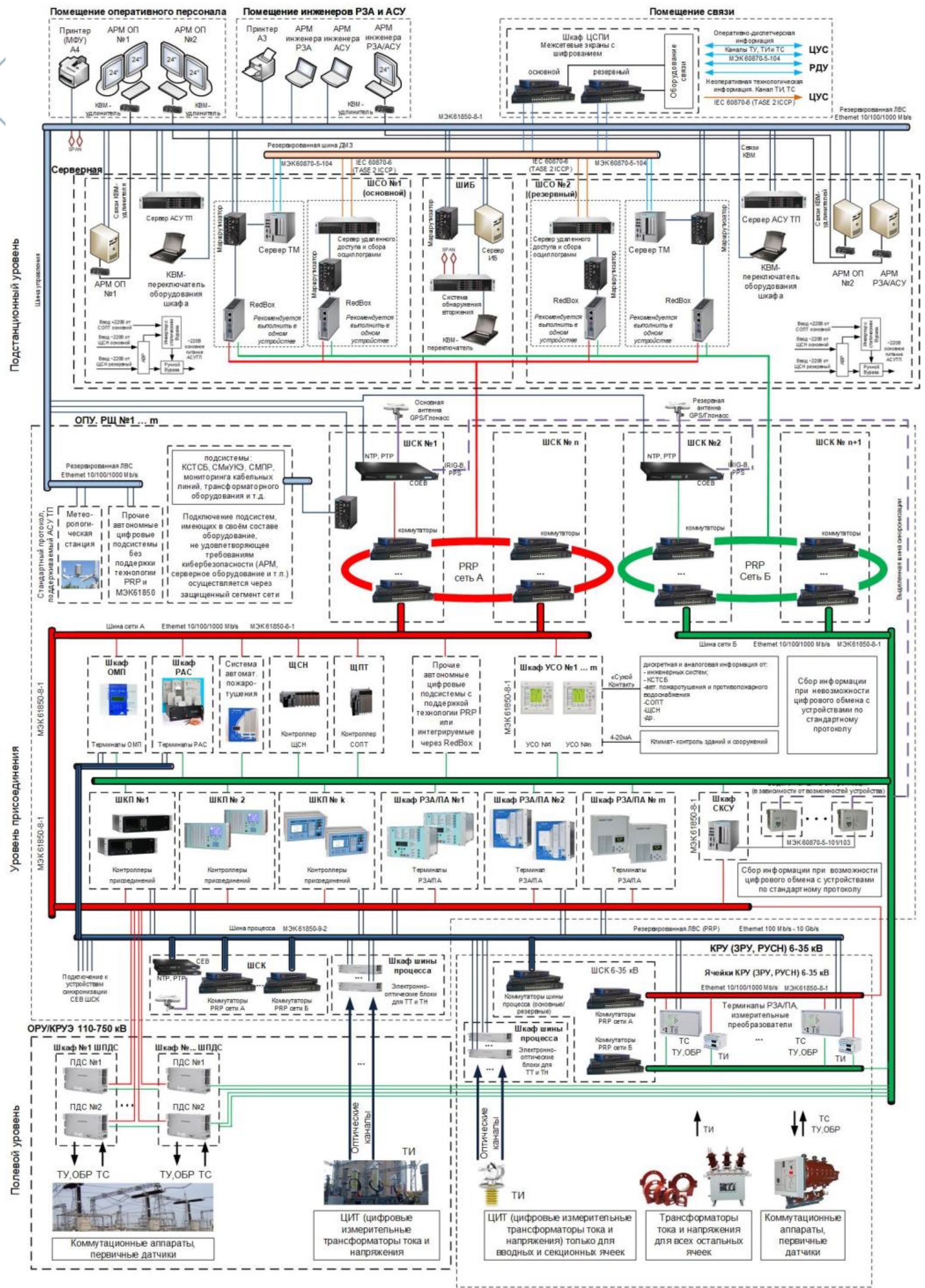
Особенности:

- для новых и реконструируемых подстанций;
- применение протокола PRP (MMS, GOOSE);
- без использования протокола SV;
- применение ШПДС;
- учет требований в части ИБ.

Проект СТО «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС»

III архитектура с отдельной шиной процесса

Структурная схема типового ПТК АСУТП с применением стандарта МЭК 61850-9-2



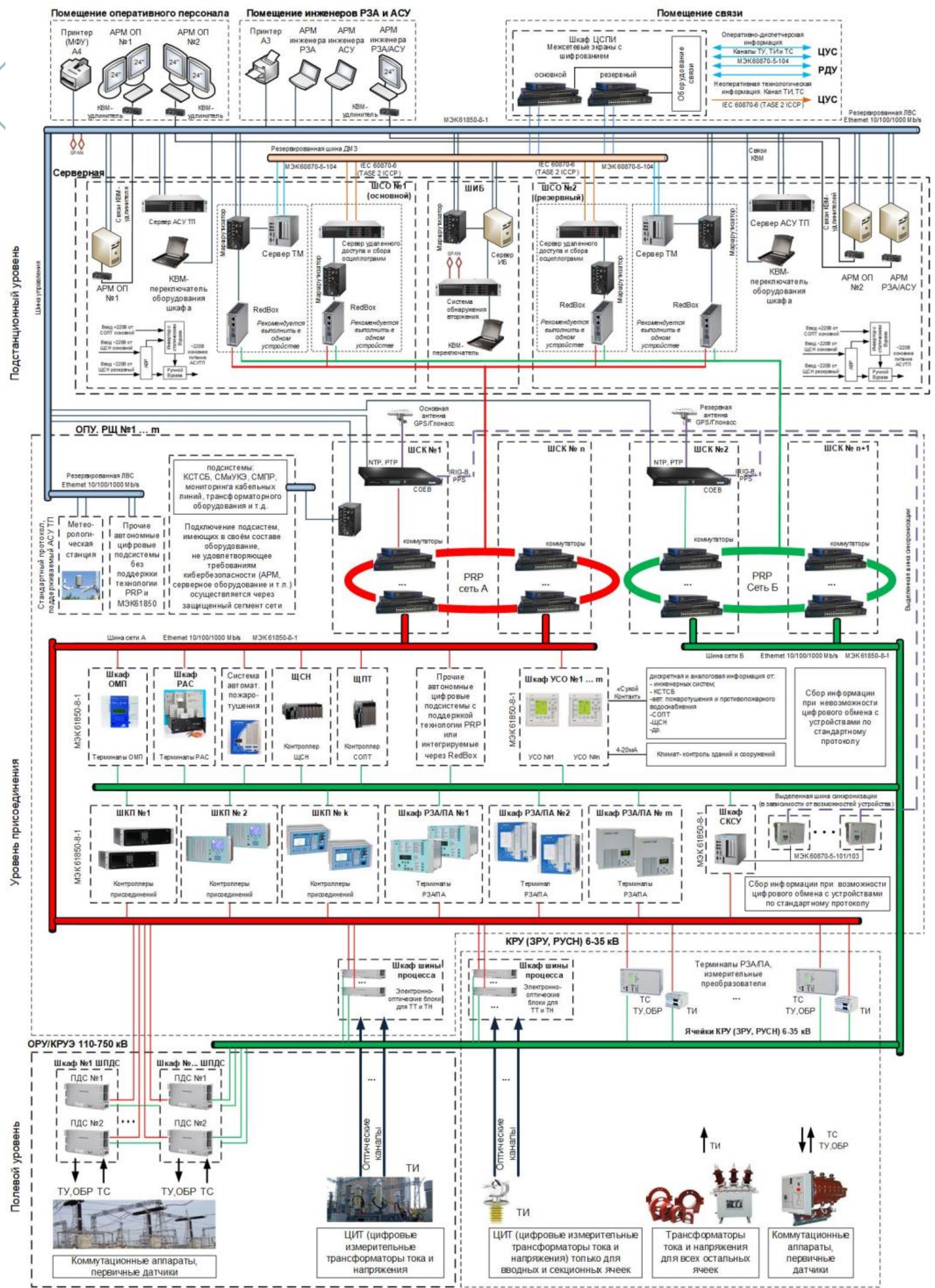
Помещение оперативного персонала
Помещение инженеров РЗА и АСУ
Помещение связи
Принтер (МФУ) А4
АРМ ОП №1
АРМ ОП №2
Принтер А3
АРМ инженера РЗА
АРМ инженера АСУ
АРМ инженера РЗА/АСУ
КВМ - удлинитель
Шкаф ЦСПИ
Межсетевые экраны с шифрованием
основной
резервный
Оборудование связи
Оперативно-диспетчерская информация
Каналы ТУ, ТИ и ТС
МЭК 60870-5-104
Неоперативная технологическая информация. Канал ТИ, ТС
IEC 60870-6 (TASE 2 ICCP)
ЦУС
РДУ
МЭК61850-8-1
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
Резервированная шина ДМЗ
Серверная
Подстанционный уровень
Шина управления
Сервер АСУ ТП
Сервер ТМ
Сервер удаленного доступа и сбора осциллограмм
Маршрутизатор
RedBox
Рекомендуется выполнить в одном устройстве
ШСО №1 (основной)
ШСО №2 (резервный)
ШИБ
Сервер ИБ
Система обнаружения вторжения
КВМ-переключатель оборудования шкафа
АРМ ОП №2
АРМ РЗА/АСУ
Связи КВМ
ОПУ, РЩ №1 … m
Основная антенна GPS/Глонасс
Резервная антенна GPS/Глонасс
ШСК №1
ШСК № n
ШСК №2
ШСК № n+1
NTP, PTP
IRIG-B PPS
СОЕВ
коммутаторы
PRP сеть А
PRP Сеть Б
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
подсистемы: КСТСБ, СМиУКЭ, СМПР, мониторинга кабельных линий, трансформаторного оборудования и т.д.
Подключение подсистем, имеющих в своём составе оборудование, не удовлетворяющее требованиям кибербезопасности (АРМ, серверное оборудование и т.п.) осуществляется через защищенный сегмент сети
Метео-рологи-ческая станция
Прочие автономные цифровые подсистемы без поддержки технологии PRP и МЭК61850
Шина сети А Ethernet 10/100/1000 Mb/s МЭК61850-8-1
Шина сети Б Ethernet 10/100/1000 Mb/s МЭК61850-8-1
Шкаф ОМП
Шкаф РАС
Система автоматического пожаротушения
ЩСН
ЩПТ
Прочие автономные цифровые подсистемы с поддержкой технологии PRP или интегрируемые через RedBox
Шкаф УСО №1 … m
Терминалы ОМП
Терминалы РАС
Контроллер ЩСН
Контроллер СОПТ
УСО №1
УСО №n
Сбор информации при невозможности цифрового обмена с устройствами по стандартному протоколу
Климат-контроль зданий и сооружений
Уровень присоединения
ШКП №1
ШКП № 2
ШКП № k
Шкаф РЗА/ПА №1
Шкаф РЗА/ПА №2
Шкаф РЗА/ПА № m
Шкаф СКСУ
Контроллеры присоединений
Терминалы РЗА/ПА
МЭК 60870-5-101/103
Сбор информации при возможности цифрового обмена с устройствами по стандартному протоколу
Шина процесса МЭК61850-9-2
Резервированная ЛВС (PRP) Ethernet 100 Mb/s - 10 Gb/s
Подключение к устройствам синхронизации СЕВ ШСК
ШСК
Коммутаторы PRP сети А
Коммутаторы PRP сети Б
Шкаф шины процесса
Электронно-оптические блоки для ТТ и ТН
КРУ (ЗРУ, РУСН) 6-35 кВ
ШСК 6-35 кВ
Ячейки КРУ (ЗРУ, РУСН) 6-35 кВ
Терминалы РЗА/ПА, измерительные преобразователи
ТС ТУ,ОБР
ТИ
ОРУ/КРУЭ 110-750 кВ
Шкаф №1 ШПДС
Шкаф №… ШПДС
ПДС №1
ПДС №2
ТУ,ОБР ТС
Полевой уровень
Оптические каналы
Коммутационные аппараты, первичные датчики
ЦИТ (цифровые измерительные трансформаторы тока и напряжения
ЦИТ (цифровые измерительные трансформаторы тока и напряжения) только для вводных и секционных ячеек
Трансформаторы тока и напряжения для всех остальных ячеек
Коммутационные аппараты, первичные датчики

Особенности:

- для новых и реконструируемых подстанций;
- применение протокола PRP (MMS, GOOSE);
- отдельная шина процесса для SV-потоков;
- применение ШПДС;
- применение цифровых измерительных ТТ и ТН;
- применение электронно-оптических блоков для ТТ и ТН;
- учет требований в части ИБ.

Проект СТО «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС»

III архитектура с мультишиной


Структурная схема типового ПТК АСУТП с применением стандарта МЭК 61850-9-2

Помещение оперативного персонала
Принтер (МФУ) А4
АРМ ОП №1
АРМ ОП №2
КВМ-удлинитель
Помещение инженеров РЗА и АСУ
Принтер А3
АРМ инженера РЗА
АРМ инженера АСУ
АРМ инженера РЗА/АСУ
Помещение связи
Шкаф ЦСПИ
Межсетевые экраны с шифрованием
основной
резервный
Оборудование связи
Оперативно-диспетчерская информация
Каналы ТУ, ТИ и ТС
МЭК60870-5-104
ЦУС
РДУ
Неоперативная технологическая информация. Канал ТИ, ТС
IEC 60870-6 (TASE 2 ICCP)
МЭК61850-8-1
Резервированная ЛВС Ethernet 10/100/1000 Mb/s
SPAN
Резервированная шина ДМЗ
Серверная
Связи КВМ-удлинителя
Сервер АСУ ТП
КВМ-переключатель оборудования шкафа
ШСО №1 (основной)
ШИБ
ШСО №2 (резервный)
Маршрутизатор
Сервер ТМ
Сервер удаленного доступа и сбора осциллограмм
Сервер ИБ
Система обнаружения вторжения
КВМ-переключатель
RedBox
Рекомендуется выполнить в одном устройстве
Связи КВМ
АРМ РЗА/АСУ
Ввод ~220В от СОПТ основной
Ввод ~220В от ЩСН основной
Ввод ~220В от ЩСН резервный
АВР
Инвертор с статическим байпасом
Ручной байпас
~220В основное питание АСУТП
Подстанционный уровень
Шина управления
ОПУ, РЩ №1 … m
Основная антенна GPS/Глонасс
Резервная антенна GPS/Глонасс
ШСК №1
ШСК № n
ШСК №2
ШСК № n+1
NTP, PTP
IRIG-B, PPS
СОЕВ
коммутаторы
PRP сеть А
PRP Сеть Б
Выделенная шина синхронизации
подсистемы: КСТСБ, СМиУКЭ, СМПР, мониторинга кабельных линий, трансформаторного оборудования и т.д.
Подключение подсистем, имеющих в своём составе оборудование, не удовлетворяющее требованиям кибербезопасности (АРМ, серверное оборудование и т.п.) осуществляется через защищенный сегмент сети
Стандартный протокол, поддерживаемый АСУ ТП
Метеорологическая станция
Прочие автономные цифровые подсистемы без поддержки технологии PRP и МЭК61850
Шина сети А
Ethernet 10/100/1000 Mb/s
Шина сети Б
Шкаф ОМП
Терминалы ОМП
Шкаф РАС
Терминалы РАС
Система автомат. пожаротушения
ЩСН
Контроллер ЩСН
ЩПТ
Контроллер СОПТ
Прочие автономные цифровые подсистемы с поддержкой технологии PRP или интегрируемые через RedBox
Шкаф УСО №1 … m
УСО №1
УСО №n
«Сухой Контакт»
4-20мА
дискретная и аналоговая информация от:
- инженерных систем;
- КСТСБ
-авт. пожаротушения и противопожарного водоснабжения
-СОПТ
-ЩСН
-др.
Климат-контроль зданий и сооружений
Сбор информации при невозможности цифрового обмена с устройствами по стандартному протоколу
ШКП №1
ШКП № 2
ШКП № k
Контроллеры присоединений
Шкаф РЗА/ПА №1
Шкаф РЗА/ПА №2
Шкаф РЗА/ПА № m
Терминалы РЗАПА
Терминал РЗАПА
Шкаф СКСУ
Выделенная шина синхронизации (в зависимости от возможностей устройства)
МЭК60870-5-101/103
Сбор информации при возможности цифрового обмена с устройствами по стандартному протоколу
Уровень присоединения
КРУ (ЗРУ, РУСН) 6-35 кВ
Шкаф шины процесса
Электронно-оптические блоки для ТТ и ТН
Терминалы РЗА/ПА, измерительные преобразователи
ТС
ТУ,ОБР
ТИ
Ячейки КРУ (ЗРУ, РУСН) 6-35 кВ
ОРУ/КРУЭ 110-750 кВ
Шкаф №1 ШПДС
Шкаф №… ШПДС
ПДС №1
ПДС №2
Оптические каналы
Полевой уровень
Коммутационные аппараты, первичные датчики
ЦИТ (цифровые измерительные трансформаторы тока и напряжения
ЦИТ (цифровые измерительные трансформаторы тока и напряжения) только для вводных и секционных ячеек
Трансформаторы тока и напряжения для всех остальных ячеек
Коммутационные аппараты, первичные датчики

Особенности:

- для новых и реконструируемых подстанций;
- применение протокола PRP (MMS, GOOSE);
- объединение MMS-, GOOSE- и SV-потоков в мультишине;
- применение ШПДС;
- применение цифровых измерительных ТТ и ТН;
- применение электронно-оптических блоков для ТТ и ТН;
- учет требований в части ИБ.

Выводы

1. Внедрение СТО позволит привести функционал ЛВС АСУ ТП в соответствие с НПА РФ.

2. Проектирование цифровых подстанций на основе данного СТО позволит типизировать решения и навести «порядок» в проектной документации.

3. Повысить эксплуатационные характеристики систем управления цифровых подстанций.

Спасибо за внимание!

Максим Никандров
ООО «Интеллектуальные Сети»
nikandrov@igrids.ru