Особенности информационной безопасности АСУТП электростанций на базе современных программно-технических комплексов

Профессор, д.т.н. Аракелян Э.К.
Профессор, д.т.н. Минзов А.С.

Национальный исследовательский институт МЭИ
Москва, 2014

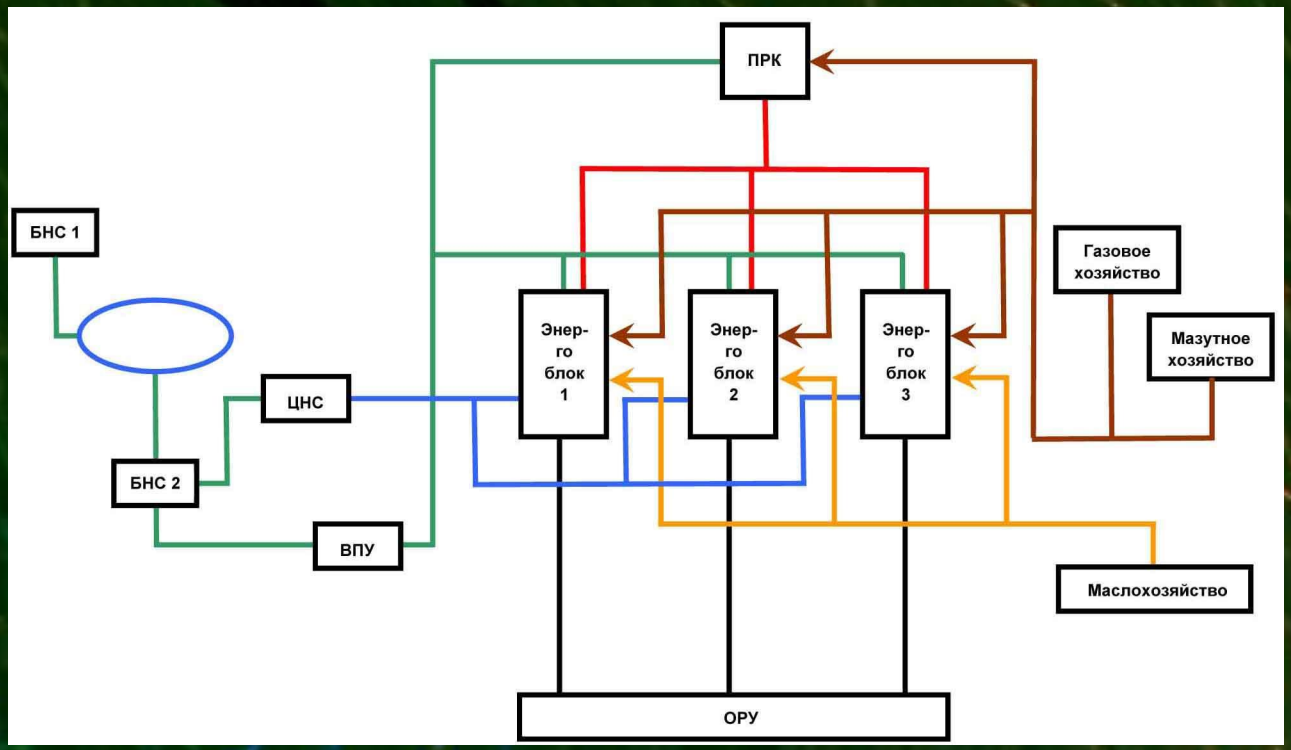
Общие положения

- Современный этап развития отечественной энергетики, как и других отраслей промышленности РФ, характеризуется широким внедрением многофункциональных АСУТП, что объективно обусловлено развитием научно-технического прогресса в области освоения новых информационных технологий и постоянным совершенствованием микропроцессорных аппаратно-технических средств контроля и управления, сетевых средств обмена информацией и передачей управляющих команд.
- Современная ТЭС – сложный объект управления, состоящий из большого числа взаимосвязанных по технологическому процессу агрегатов. Технологический процесс ТЭС и АЭС отличается сложностью взаимосвязей между большим числом агрегатов, высокими параметрами рабочей среды, жесткими требованиями к точности их регулирования.
- Любая комплексная или полномасштабная АСУТП представляет собой сложную систему, зависящую от степени автоматизации технологического объекта и всей электростанции в целом и охватывает как тепломеханическое, так и электротехническое оборудование.

Общие положения

- Современные АСУТП перестали быть вспомогательными средствами производственного процесса и служат в настоящее время: системой сбора и отображения информации в режиме текущего времени (on-line), автоматизированного анализа происходящих процессов, и управления всеми режимами работы основного и вспомогательного оборудования ТЭС на блочном уровне и производственными процессами на станционном уровне .
- Основным элементом АСУТП является базовый программно-технический комплекс (ПТК), в котором все технические средства, связаны разветвленной сетевой иерархической структурой.

Упрощенная структура современной Тепловой электростанции



Основные тенденции развития АСУТП

- Модернизация существующих и создание новых АСУТП на базе ПТК, в том числе зарубежного производства;
- Тенденция к поставке оборудования со своей локальной системой контроля и управления, выполненные на различных технических средствах;
- Значительная доля оборудования и ПТК зарубежного производства, особенно в последние годы, при широком внедрении новых технологий производства энергии на базе ГТУ и ПГУ;
- Переход на цифровую передачу информации; создание цифровых промышленных сетей, беспроводных систем передачи информации;
- Развитие территориально-распределенных АСУТП с установкой полевых контроллеров;
- Интеллектуализация измерительных устройств и запорно-регулирующей арматуры;
- Переход на создание единой системы управления технологическими и производственными процессами во всех режимах работы энергоблоков и станции в целом;

Основные тенденции развития управления электростанциями

- Переход энергетики на рыночные отношения привело к:

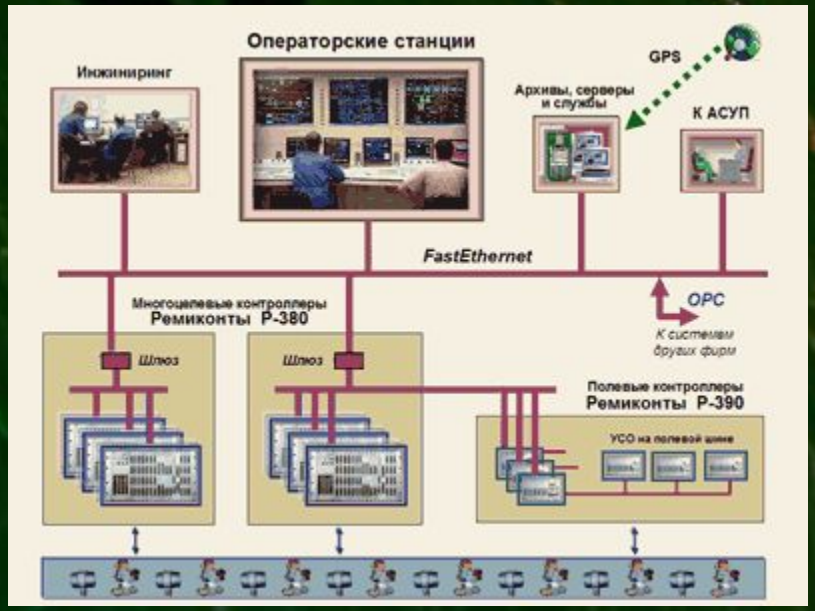
  - созданию большого количества управляющих компаний (ОГК, ТГК и т.д.) со своими корпоративными сетями и с удаленным доступом к станциям (в основном - телефон, интернет);

  - необходимости передачи большого объема информации со станционного уровня на уровень управления энергосистемой и обратно (в основном по интернету);

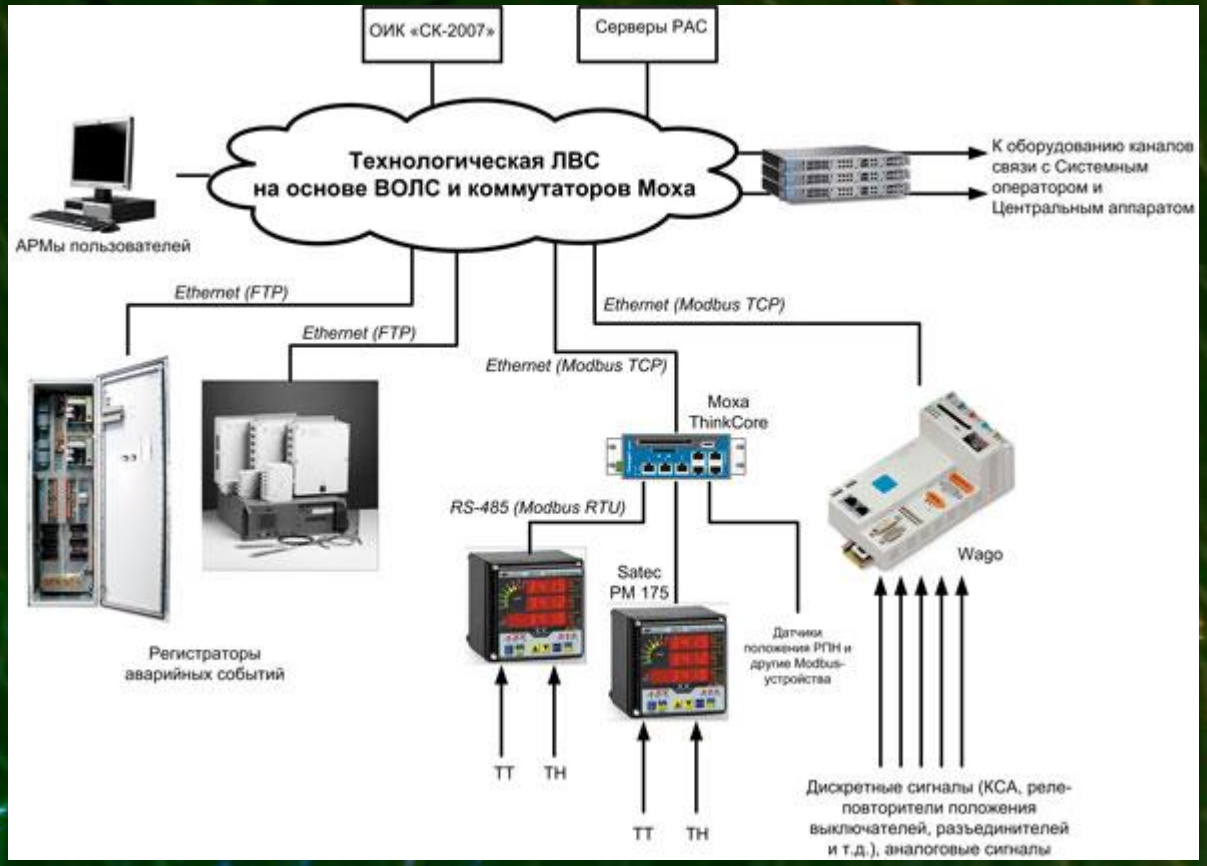
  - оперативного управления текущих режимов со стороны СО-ЦДУ (РДУ) - (по интернету);

- Разработки Систем обмена технологической информацией с Автоматизированной системой Системного оператора (СОТИ АССО) для измерения параметров электрооборудования главной схемы электростанции, сбора телемеханической информации и передачи её на диспетчерские пункты филиалов СО ЕЭС.

Упрощенная структура распределенной АСУТП ТЭС (на базе ПТК «Квинт»)



Пример структурной схемы (СОТИ АССО ОАО «Концерн Энергоатом»



Атаки на системы управления

По данным фирмы Schneider Electric, 2011г.

- Через корпоративный WAN и коммерческую сеть (в том числе инфицированные ноутбуки) – 47%;
- Через Интернет – 17%;
- Через VPN – 7%;
- Через телефонный модем – 7%;
- Через разрешенные сети партнеров – 10%;
- Через сеть Telco – 7 %;
- Через беспроводную связь – 3%.

Некоторые выводы из анализа состояния АСУТП

- Основная особенность развития электроэнергетики в РФ заключается в ее технической и технологической зависимости от зарубежных стран.
- Современная АСУТП электростанций имеет сильно разветвленную иерархическую информационную сеть.
- Следовательно, концепцию защиты АСУТП объектов энергетики необходимо строить из условия создания безопасных автоматизированных систем, работающих в **недоверенной** среде.

Некоторые проблемы ИБ АСУТП ТЭС

- 1. Низкий уровень ИБ на всех иерархических уровнях управления
- 2. Недопонимание заказчиков АСУТП значимости проблемы ИБ;
- 3. Отсутствие четких методических положений учета ИБ на этапе проектирования АСУТП;
- 4. Отсутствие специалистов по ИБ с базовым образованием АСУТП.

Основные пути решения этой проблемы (1)

1. Разработка типовых сценариев скрытого управления АСУТП, которые должны быть классифицированы, постоянно обновляться и использоваться при оценке эффективности противодействия системы защиты АСУТП технологиям скрытого управления.

2..Требуется разработка новых концептуальных и методологических подходов к защите АСУТП, так как существующая нормативная база по обеспечению информационной безопасности КВО не в полной мере учитывает возможные целенаправленные изменения информации от датчиков, PLC и логику технологических процессов электростанций.

Основные пути решения этой проблемы (2)

3. Одним из инновационных направлений по защите АСУТП является концепция упреждающий или ***проактивной защиты,*** когда управление объектом энергетики проводится одновременно с анализом состояния системы информационной безопасности АСУТП и системы управления объектом энергетики с последующим моделированием его будущего состояния от очередного управляющего воздействия.

Основные пути решения этой проблемы (3)

4. Другой подход к защите АСУТП основан на идее ***активной*** защиты путем создания механизмов доверия к элементам АСУТП за счет мониторинга их состояния и анализа логики процессов. Это потребует изменения технологий проектирования АСУТП:

системы безопасности КВО должны будут проектироваться совместно с технологическими процессами.

Основные пути решения этой проблемы (4)

5. Весьма перспективной, на наш взгляд, является концепция обеспечения безопасности АСУТП на различных этапах жизненного цикла, основанная на идее ***активной защиты на основе контроля поведенческой модели*** (авторы концепции - ***ИПУ РАН)***

Основные пути решения этой проблемы (5)

6.Требуется научная проработка и подготовка проекта ФЗ ***"О безопасности критически важных объектов инфраструктуры РФ***", в котором должны быть представлены принципы и механизмы защиты КВО, разделение ответственности государства и собственников хозяйствующих субъектов КВО, основные функции и структура государственной системы контроля состояния безопасности КВО.

Основные пути решения этой проблемы (6)

7. В условиях постоянного роста киберугроз для объектов энергетики, относящихся к критически важным, требуется введения в направление высшего профессионального образования ***«Информационная безопасность»*** нового профиля подготовки бакалавров и магистров ***"Информационная безопасность КВО"***.

- СПАСИБО ЗА ВНИМАНИЕ