

Как обеспечить сбор данных в/из АСУ ТП без курсов программирования и проблем с безопасниками

Машинский Юрий Викторович

заместитель директора Инженерного
центра АО «ЭЛАРА».

Круглый стол «Импортозамещение для цифровизации
энергетической отрасли»
ТЭФ-2023



АО «ЭЛАРА» - российский производитель и разработчик комплексных решений для автоматизации

Более 20 лет создаем АСУ ТП для крупнейших промышленных и энергетических компаний

- Системообразующее предприятие федерального уровня;
- Год основания – 1970;
- Ключевые отрасли – авионика, АСУ ТП, железнодорожный транспорт, автомобилестроение;
- Собственное производство от изготовления печатных плат до сервисного обслуживания;
- Современное производство площадью более 120 000 м²;
- Более 4000 сотрудников;
- Полный цикл производства от изготовления печатных плат до заводских испытаний АСУ ТП;
- Собственный испытательный центр;
- Развитая служба сервиса с опытом работы в различных регионах России и мира;
- Качество продукции подтверждено российскими и международными сертификатами.



Если информация из АСУ ТП не используется в бизнес-процессах предприятия, значит предприятие теряет деньги!

Технические задачи

- Диспетчерское управление;
- Интеграция локальных САУ;
- Передача информации надзорным органам.

Бизнес задачи, решаемые с помощью данных АСУ ТП:

- Сокращение стоимости обслуживания отдельных систем автоматики;
- Сокращение времени простоя оборудования на выявление отказов, на переключения – повышение коэффициента полезного использования;
- Повышение качества обслуживания клиентов;
- Сокращение брака ...

Распространенные инструменты интеграции

УСПД и серверы телемеханики:

- Сильно специализированы;
- Ограничены в поддержке протоколов передачи информации;

Классические «OPC серверы»:

- Windows-only;
- Ограничены в поддержке протоколов передачи информации;
- Система лицензирования ограничивает возможности расширения АСУ ТП устройствами с другими типами протоколов;
- «дикая» стоимость всего кроме Modbus.

Edge/IIoT шлюзы:

- Linux-style конфигурирование – требует высокой квалификации инженеров для внедрения и эксплуатации;
- Никакая поддержка команд;
- состоит из open-source компонентов с «какой-то» надежностью и длинным хвостом зависимостей;

Собственная разработка Пользователем:

- не прогнозируемо по цене, качеству, и срокам;
- состоит из open-source компонентов с «какой-то» надежностью и длинным хвостом зависимостей;
- зарплата программистов сожрет любую экономию.

ОЕМ и open-source без внедрения БРПО это халатность или диверсия

Исправления в исходном коде компонентов ломают ваш продукт. Иногда фатально ☹

Open-source и КОММЕРЧЕСКИЕ SDK тестируются и разрабатываются только под основными операционными системами.

Количество звезд на Github не гарантирует качества продукта

Примеры из жизни:

1. НДВ в известном коммерческом SDK для OPC UA – возможность подключения к серверу OPC UA любым пользователем зарегистрированным в том же домене AD.

2. В том же SDK под Linux количество ошибок заметно больше чем под Windows.

П Р И К А З

25 декабря 2017 г.

Москва

№ 239

29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее – программное обеспечение), должно соответствовать следующим требованиям по безопасности:

29.3.1. Требования по безопасной разработке программного обеспечения:

- наличие руководства по безопасной разработке программного обеспечения;
- проведение анализа угроз безопасности информации программного обеспечения;
- ...
- проведение статического анализа **исходного кода программы**;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;

....

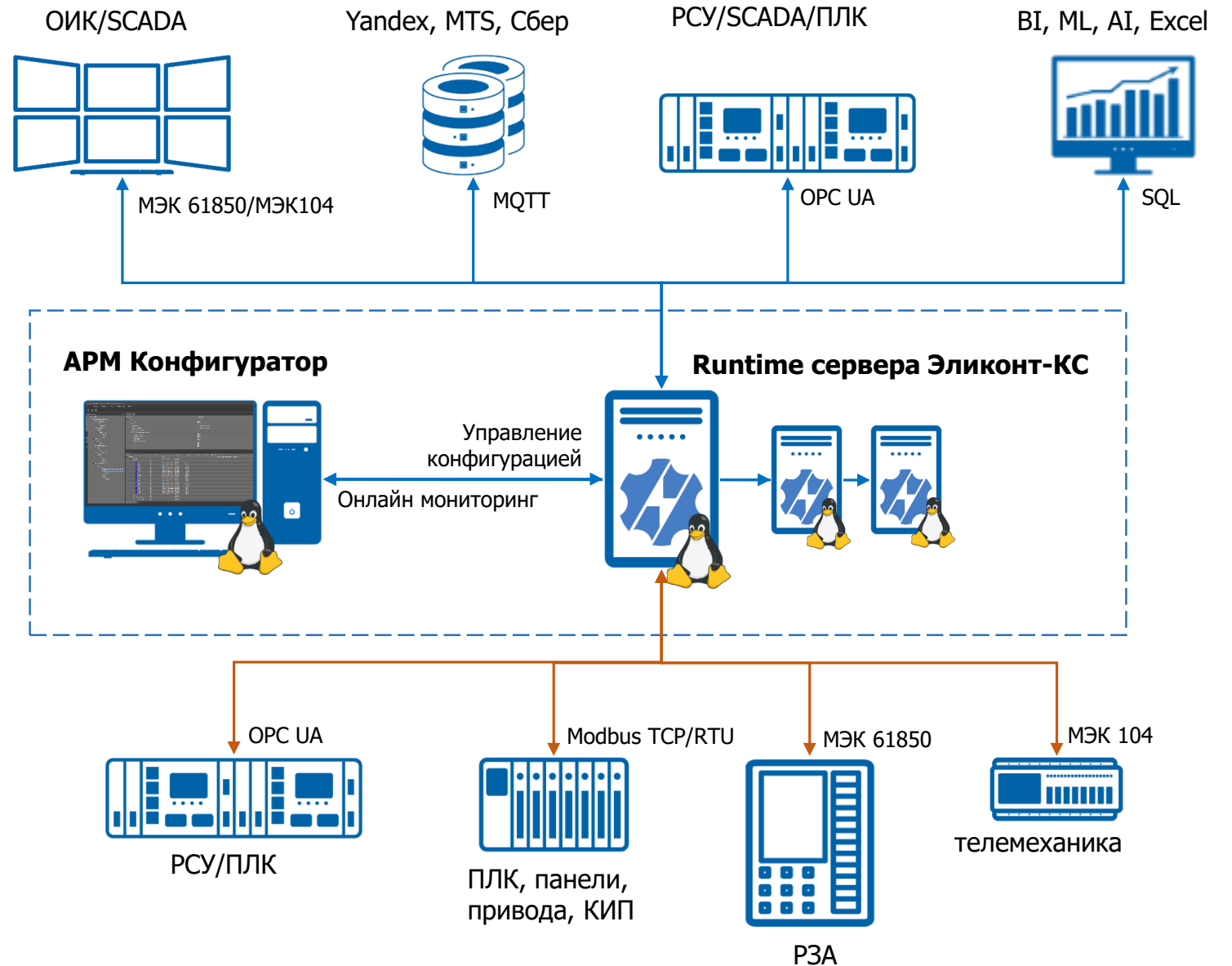
«Зашитые» учетные данные в исходном коде библиотеки OPC UA

```
// This is just a trivial example with 5 different users
if ((pUserPwToken->sUserName == "root" && pUserPwToken->sPassword == "secret") ||
    (pUserPwToken->sUserName == "joe" && pUserPwToken->sPassword == "god") ||
    (pUserPwToken->sUserName == "john" && pUserPwToken->sPassword == "master") ||
    (pUserPwToken->sUserName == "sue" && pUserPwToken->sPassword == "curly") ||
    (pUserPwToken->sUserName == "sam" && pUserPwToken->sPassword == "serious"))
{
```

Проверьте, удалены они в вашей реализации OPC UA?

«Эликонт-КС» - универсальный ответ на задачи интеграции в АСУ ТП

- Интеграция в общее коммуникационное пространство:
 - Частотных преобразователей и электроприводов;
 - ПЛК и панелей управления;
 - РЗА и телемеханики;
 - Локальных САУ и СМВД;
 - Серверов SCADA;
 - IIoT платформ и ML систем.
- Передача команд управления между различными системами;
- Хранение архивов технологических параметров;
- Поддержка Windows и Linux включая AstraLinux и ROSA



«Эликонт-КС» в реестре российского программного обеспечения



«Эликонт-КС» предоставляет выбор вариантов использования

Программное обеспечение

Варианты:

1. Дистрибутив программного обеспечения под операционные системы Linux или Windows (доступно на сайте ptk-sura.ru);
2. Настроенный контейнер или образ виртуальной машины для установки на «железо» заказчика;

Для установки **НЕ** требуется соединение с интернетом!

Конфигурируемый набор опций под проект:

Кол.Сигналов + требуемые функции(протоколы, архив и пр.)

До 100 тегов или 5 часов бесплатно для тщательного предварительного тестирования Заказчиком.

Возможность расширения лицензии после приобретения

Аппаратный или программный лицензионный ключ.

Оptionальная подписка на обновление версий ПО.

Промышленный компьютер с прикладным программным обеспечением



Встроенная мультилицензия с ограничением только по количеству сигналов - от 500 до 30 000;

Собственная сборка ОС Linux обеспечивающая перезагрузку ПК за 30 секунд;

Возможность обновления версии ПО в процессе эксплуатации;

Возможность установки Эликонт-КС на аппаратную платформу контроллера «Эликонт-100»;

Температура эксплуатации -20 ~ +70 °С.

«Эликонт-КС» сокращает трудоемкость инжиниринга особенно распределенных ССПИ с десятками серверов.

- один проект может содержать десятки коммуникационных серверов;
- предотвращает грубые ошибки в настройке;
- обеспечивает переносимость проектов;
- импорт-экспорт списков сигналов в файлы *.csv;
- импорт файлов SCL для интеграции РЗА;
- настройка трансляции команд дистанционного управления между протоколами

The screenshot displays the 'Эликонт-Конфигуратор' (Elicont Configurator) software interface. The main window is titled 'Эликонт-Конфигуратор v.0.8.0-unstable-0621179 [127.0.0.1:19000/Проект АСУТП]'. The interface is divided into several panes:

- Navigation pane (left):** Shows a tree view of the project structure under 'Проект АСУТП', including 'Коммуникационный Сервер', 'Modbus TCP клиент', 'OPC UA клиент', and 'МЭК 60870-5-104 клиент'.
- Properties pane (top right):** Shows the configuration for the selected 'rcb1111' server. It includes fields for 'Активация' (checked), 'Имя' (rcb1111), 'Адрес отчета', 'Адрес набора данных', 'Количество экземпляров', and 'Настройки формирования отчёта' (e.g., 'Изменение данных', 'Изменение качества', 'Целостность', 'Время целостности, мс', 'Общий опрос', 'Обновление данных', 'Задержка отправки, мс').
- Details pane (bottom right):** Shows a table of signal details for the selected server. The table has columns: Node, FC, Type, Value, Name, LogicalDevice, LogicalNode, DOPath, VarPath, CDC, and Desc. The signals listed include ENIP3, LD, DATA, LN, LPHD1, CSWI1-4, GGIO1, MMTR, MMXU, MSQ1, XCBR1, XSWI1-2, CIL01, and CIL02.
- Signal List Table (bottom right):** A table showing signal details with columns: Имя, Значение, Метка времени, and Качество. The signals listed include 'Коммуникационный Сервер/OPC клиент/Ethernet/Эликонт-100/Опрос/Сигналы' and 'Коммуникационный Сервер/МЭК 60870-5-104 сервер/Ethernet/LVC/Сигналы'.

Пользователь может выбирать - контроль за работой всех серверов с единого АРМ или с любого компьютера сети через Web интерфейс

Функции доступные через web-сервер коммуникационного ядра

- Авторизация пользователей
- Использование ресурсов сервера
- Контроль данных на входе и на выходе;
- Данные о лицензии;
- Выгрузка логов;
- В разработке – отображение архивных данных из встроенной БД.

The image displays two screenshots of the 'Эликонт-КС' web interface. The top screenshot shows the 'Исполнение' (Execution) page, which features a search bar with the text 'Modbus TCP клиент/Ethernet/Simulation_S' and a 'Узлы' button. Below the search bar is a table with the following data:

Наименование	Значение	Качество	Время	Тип данных
TC13_Mod_bit13 <small>Modbus TCP клиент/Ethernet/Simulation_Slave_IooСигналы</small>	1	Success	2023-04-04 08:02:58.105	BOOLEAN
TC03_Mod_bit3 <small>Modbus TCP клиент/Ethernet/Simulation_Slave/Сигналы</small>	0	Success	2023-04-04 08:38:04.868	BOOLEAN
TC15_Mod_bit15 <small>Modbus TCP клиент/Ethernet/Simulation_Slave_IooСигналы</small>	1	Success	2023-04-04 08:02:58.105	BOOLEAN
TC04_Mod_bit4 <small>Modbus TCP клиент/Ethernet/Simulation_Slave_IooСигналы</small>	1	Success	2023-04-04 08:02:58.105	BOOLEAN

The bottom screenshot shows the 'Настройки' (Settings) page, specifically the 'Пользователи' (Users) tab. It displays a list of users: 'admin', 'guest', and 'user'. The 'admin' user is selected. To the right of the list, the following information is shown:

- ID: bdcf49b7-804c-4bb4-ad71-275267644189
- Пользователь: admin
- Роль: Администратор (dropdown menu)

Below this information are two buttons: 'Изменить логин' (Change login) and 'Изменить пароль' (Change password). A dark sidebar on the left of both screenshots contains navigation options: Главная, Исполнение, Лицензия, Диагностика, Логи, Настройки, and Выход.

«Эликонт-КС» - соответствует требованиям 239 приказа ФСТЭК в части практик БРПО

В СООТВЕТСТВИИ С ГОСТ Р 56939-2016

- Разработан комплект из 30 документов от Технических условий до Журнала обучения сотрудников
- Поддерживается в актуальном состоянии перечень зависимостей для всех компонентов продукта;
- Программное обеспечение специально дорабатывается для получения возможности проведения фаззинг тестирования;
- Новые релизы сопровождаются информацией об исправленных уязвимостях;

Страницы /... / v 2.0.0

Коммуникационное ядро версии 2.0
Создатель: [redacted], отредактировано янв 17, 2023

Наименование компонента	Версия	Источник	Метод КС	Контрольная сумма
[redacted]	[redacted]	https://[redacted]	SHA-1	9dfbd34[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	1708e3e[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	2514f0b[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	caef7f1c[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	0ced4f5[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	69a111e[redacted]
[redacted]	[redacted]	https://[redacted]	SHA-1	aecba11[redacted]

Страницы /... / Перечень зависимостей и уязвимостей

v 2.0.0
Создатель: [redacted], отредактировано янв 17, 2023

Особенности релиза

- Исключен RabbitMQ.
- Проведен рефакторинг микросервисов.
- Сервис безопасности реализован на IdentityServer4.

Статус исправления уязвимостей по компонентам Эликонт-КС

Ключ	Тема	Автор	Создан	Приоритет	Severity	Исполнитель	Статус	Резолюция
CS-1494	ИБ. Уязвимости в компо[redacted]	[redacted]	фев 13, 2023	↑	Normal Normal	[redacted]	ОТКРЫТЫЙ	Не решен
CS-1493	ИБ. Уязвимости в компо[redacted]	[redacted]	фев 13, 2023	↑	Normal Normal	[redacted]	ОТКРЫТЫЙ	Не решен
CS-1449	ИБ. Уязвимости в компонен[redacted]	[redacted]	янв 17, 2023	↑	Critical Critical	[redacted]	ОТКРЫТЫЙ	Не решен
CS-1448	ИБ. Уязвимости в компо[redacted]	[redacted]	янв 17, 2023	↑	Critical Critical	[redacted]	ЗАКРЫТ	Won't Do
CS-1438	ИБ. Уязвимости в компо[redacted]	[redacted]	янв 16, 2023	↑	Normal Normal	[redacted]	ОТКРЫТЫЙ	Не решен

Пример решения с Эликонт-КС. Модернизация системы раннего обнаружения брака.

Бизнес задача:

Уменьшить потери дорогостоящих материалов, которые расходуются на дефектные экземпляры продукции.

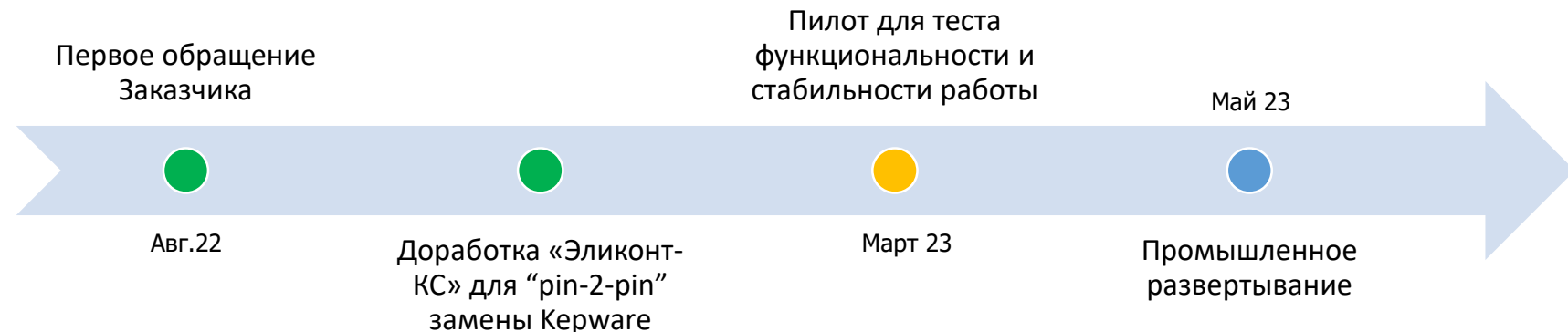
Технологическое решение:

Максимально точно и быстро локализовать границы дефекта и предотвратить дальнейшую обработку продукции.

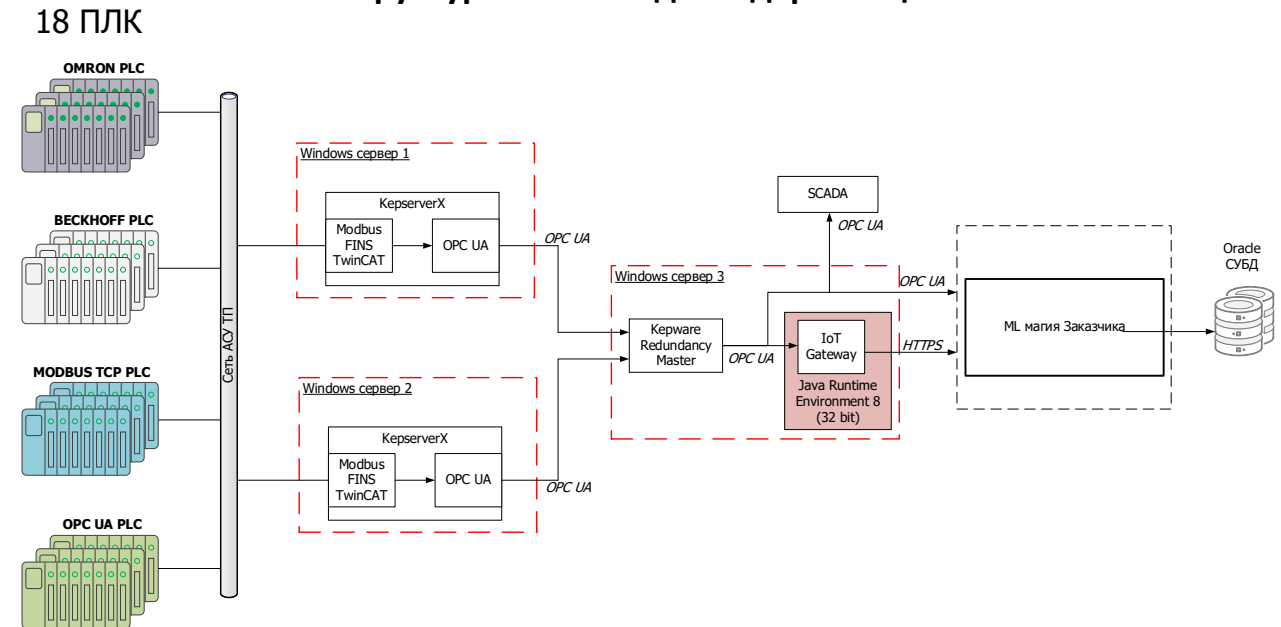
Проблемы существующей реализации:

- невозможно продлить подписку на иностранный Kerware server;
- технологи просят повысить частоту опроса ПЛК до 100 мс, при этом нагрузка на OPC сервер превысит 50 000 изменений в секунду;
- Необходимость масштабирования решения на новую площадку.

План реализации проекта:



Структура системы до модернизации



Пример решения. Модернизация системы раннего обнаружения брака.

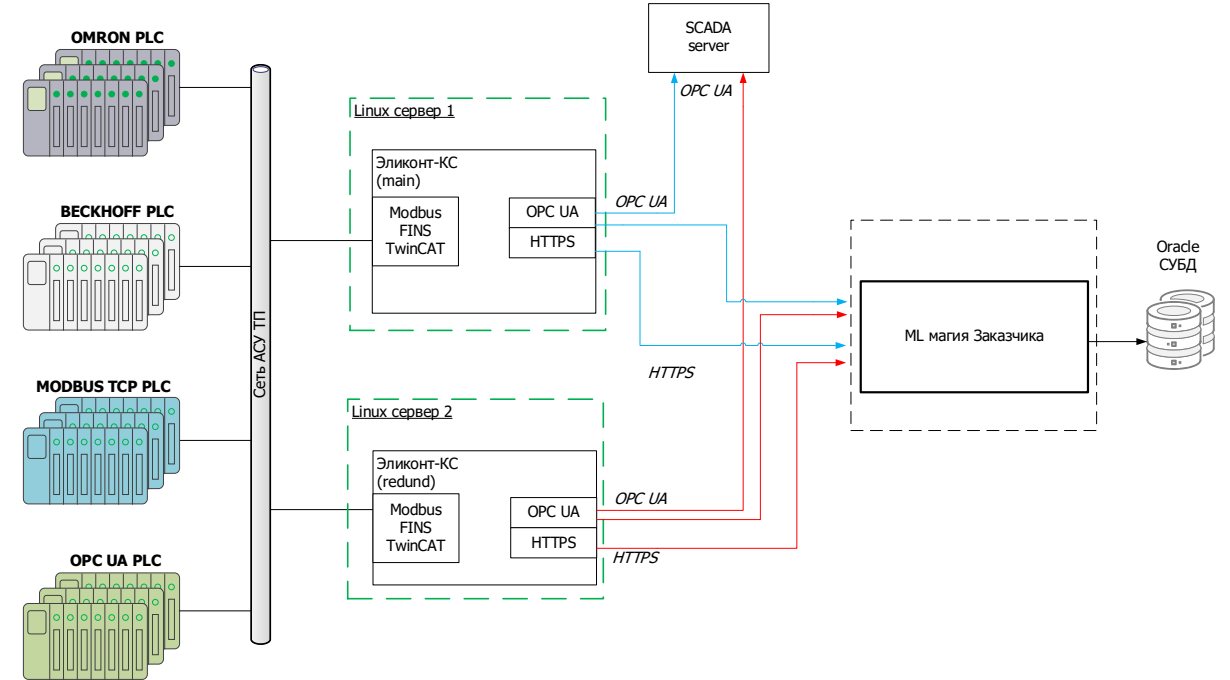
Достигнутые результаты:

- повторен используемый функционал Kerware Server;
- разработана утилита для миграции проекта из Kerware в Эликонт-КС;
- повышена точность определения границ дефектных участков за счет изменения дискретности сбора данных с 1 до 0,1 секунды;

Дополнительные выгоды:

- обеспечена возможность обновления компонентов системы без перезагрузки серверов;
- выявлен ряд «костылей» в неизменяемой части системы, ликвидация которых снизит нагрузку на ПЛК и SCADA;
- повышена надежность работы АСУ ТП за счет полноценного резервирования связей со SCADA;
- уменьшена зависимость АСУ ТП от ОС Windows;
- убраны «лишние» компоненты;
- обеспечена оперативная тех. поддержка.

Целевая структура системы после модернизации



Контакты для продолжения общения:

Инженерный центр АО «ЭЛАРА»

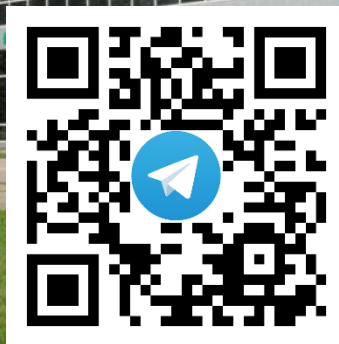
г. Москва ул. Образцова, д. 7

+7 (499) 951-08-45

inc@msk.elara.ru



ptk-sura.ru



@ptk_sura



@ptk-sura



ПТК "СУРА"

