Схемы архитектуры в разных проекциях:

- C4 Level 1 (Context)
- ML Infrastructure
- DMZ Infrastructure
- Integration Level
- C4 Level 2 (Container)
- Security Level

Цель: Разработка предложения по ИТ-решению, обеспечивающего отказоустойчивость, кибербезопасность и автономность бизнес-критичного процесса отгрузки нефтепродуктов при полной изоляции завода от корпоративной ИТ-инфраструктуры.

Решение: локализовать необходимую для процесса ИТ-инфраструктуру на территории предприятия в локальной сети.

Необходимые для поддержания работы процесса модули:

- Сервер 1С
- Бекенд оператора
- AI-сервисы (поиск аномалий в данных, мониторинг сети, распознавание документов)
- Почтовый сервер
- ПО датчиков (приемник сигналов)
- Сервис авторизации / аутентификации
- Сервис СКУД
- БД (Селена, Pangolin)
- Модуль репликации в центральный ЦОД

Отказоустойчивость: для упрощения горизонтальной масштабируемости как IT-мощностей, так и отдельных модулей, принято решение развернуть на территории предприятия IT-кластер, а сами модули запускать на виртуальных машинах. Такой подход позволяет также гарантировать отказоустойчивость достаточного уровня средствами слоя виртуализации и гибко настраивать мощности, выделенные под конкретные модули.

Кибербезопасность: от вторжения из внешней сети во внутренний контур предприятия и изоляции центрального ЦОД предусмотрена демилитаризованная зона, в которой происходит валидация входящих и выходящих пакетов. Внутренний контур зашищен несколькими компонентами:

- AI-анализ активности во внутренней сети
- AI-анализ бизнес метрик с целью детекции следствий вторжений
- Многообразие политик безопасности
- Контроль уровней физического и сетевого доступа
- SSO
- Регулярная ротация токенов
- Защита почты от фишинга, вейлинга и т.д.
- Мониторинг состояния локального кластера

Автономность: вся необходимая ИТ инфраструктура локализована на предприятии, а накопленные в процессе работы регулярно реплицируются в центральный ЦОД. При необходимости изоляции предприятия обрывается лишь тракт репликации в центральный ЦОД, что не влияет на модули, завязанные в бизнес-критичном процессе.