Робот-доставщик

Контекст

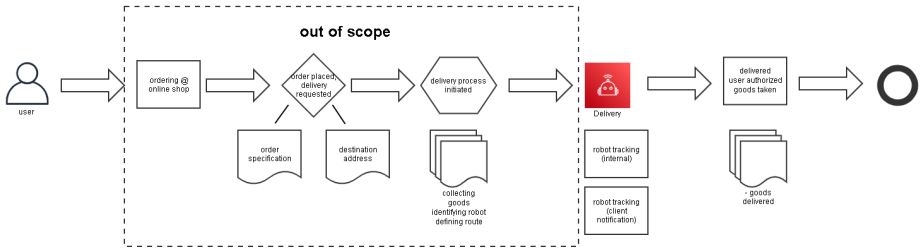
Функция

Доставка заказа клиенту на дом.

Способ доставки

С использованием самодвижущегося робота

Бизнесс процесс

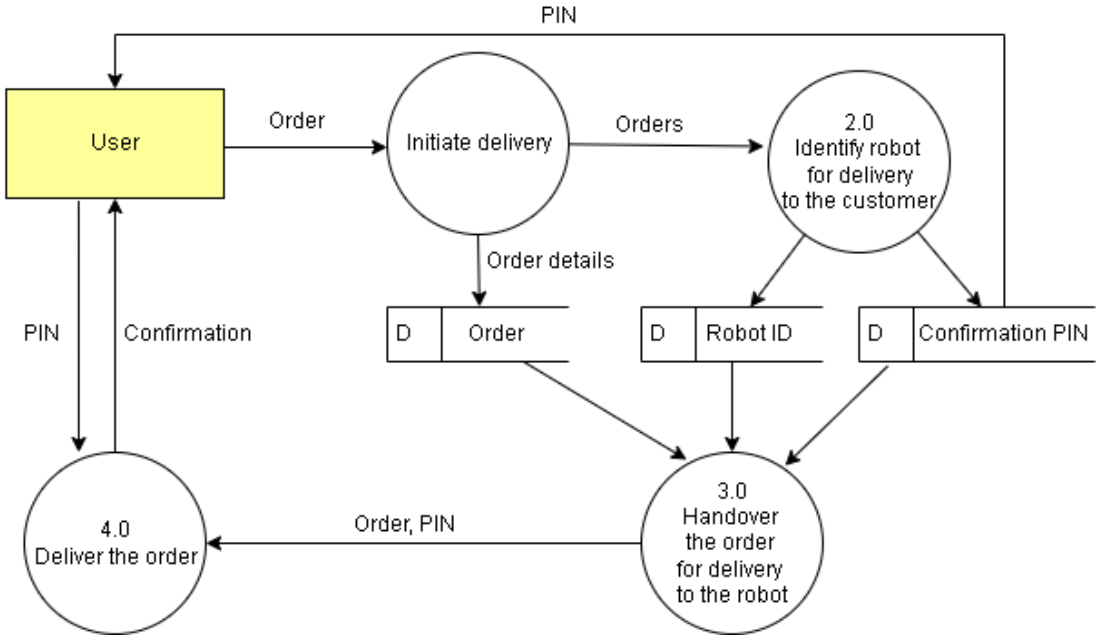


DFD (Data flow diagram)

Level 0

Level 0 DFD

ordering and delivery data flow



Цели и предположения безопасности

Цель безопасности робота

- обеспечение сохранности груза до момента передачи авторизованному клиенту
- получение задания только от корпоративного сервера
- в случае многократных попыток неавторизованного доступа вернуть груз на склад

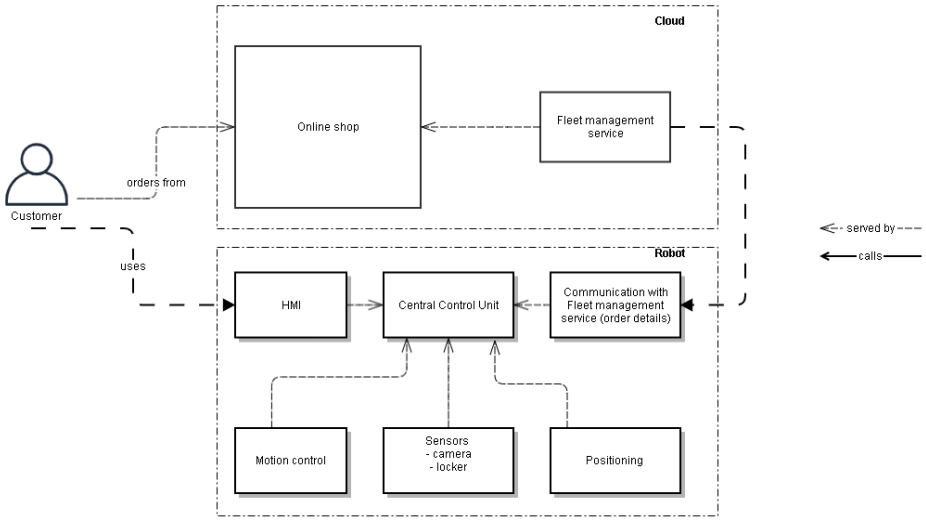
Предположения безопасности

целями безопасности робота не являются

- защита от атак с использованием физического доступа

Архитектура решения (только для учебных целей)

Функциональные компоненты портала и возможная архитектура бортового ПО робота



В рамках игры предлагается создать прототип решения, для простоты компонентам следует использовать одинаковый подход передачи сообщений (message bus), для робота следует ограничиться компонентами, собранными в группу Robot и имитатором Fleet management service из группы Cloud.

Постановка задачи

- доработать архитектуру решения при необходимости (обнаружены важные для выполнения бизнес-функции компоненты)
- разработать документ ЦПБ
- определить доверенные компоненты
- на уровне архитектуры определить механизмы обеспечения ИБ, в частности
    - защита от несанкционированного доступа к содержимому заказа, доставляемого клиенту
        - обеспечение целостности информации о заказе (адрес доставки, PIN)
        - защита от множественных попыток авторизации
- реализовать прототип решения, в ходе которого
    - "робот" получает задание на доставку с параметрами доставки (координаты, PIN)
    - имитация сервиса доставки выдаёт информацию "приехал/не приехал" в консоль (механизм автоматического уведомления пользователя о прибытии робота не требуется)
    - робот рассчитывает движение, осуществляет его с учётом ограничений и прибывает в место назначения
    - также после состояния "приехал" через HMI пользователь может ввести PIN код для получения доступа к хранилищу
    - если робот прибыл в место назначения и получил правильный PIN код, срабатывает имитация открытия хранилища (информация отображается в консольном окне)
    - после "выдачи заказа" робот должен вернуться на склад и передать статус "доставлено" серверу
    - в случае ошибки робот, не открывая хранилище, должен вернуться на склад и передать серверу статус "ошибка"

Требования

- заказ должен быть доставлен по координатам места назначения
- заказ может быть выдан клиенту только в месте назначения
- для получения доступа к заказу клиент должен ввести PIN код
- если верный PIN код не введён, заказ должен быть возвращён на склад
- все попытки несанкционированного доступа должны быть зафиксированы в системе журналирования

Критерии оценки

- функционал решения достаточен для отработки всего сценария из постановки задачи
- определены политики безопасности для взаимодействия сервисов
- неавторизованные запросы регистрируются и блокируются
- в мониторе безопасности можно отследить всю цепочку взаимодействия сервисов

Упрощения

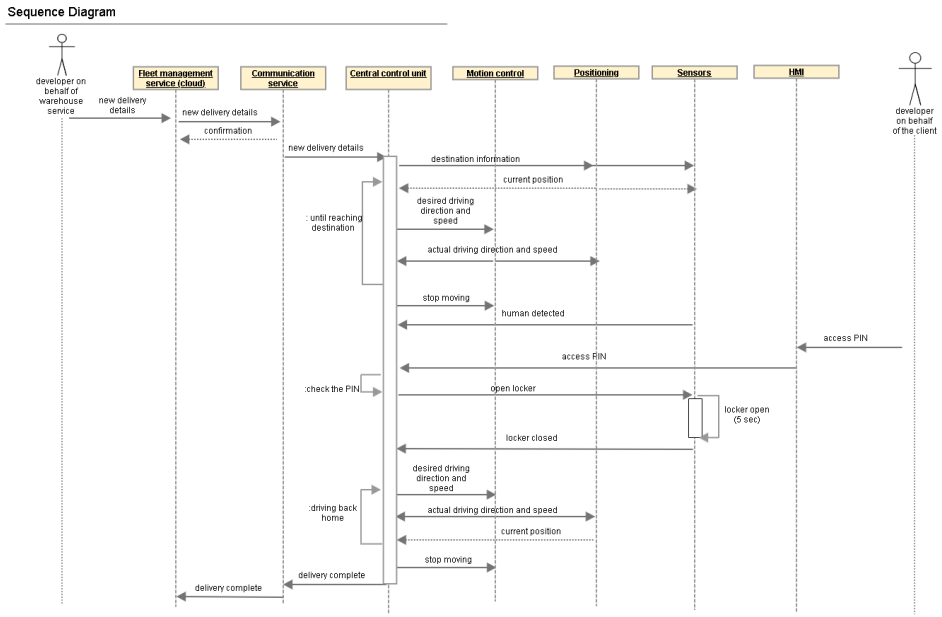
- любой товар не имеет массы и объёма, можно заказать любое количество любых товаров (в пределах доступности) в одну доставку

- графический интерфейс для взаимодействия с пользователем не требуется, достаточно примеров REST запросов (Postman коллекцией или .rest файлом в Visual Studio Code)

Принципиальные соображения

- после получения задания робот функционирует автономно (т.е. движется к клиенту, авторизует и выдаёт заказ даже в отсутствие связи с сервером)
- после доставки робот должен вернуться в пункт отправления, только тогда его задача считается выполненной

Последовательность шагов выполнения заказа роботом-доставщиком



Подсистемы

Клиент (Customer)

- взаимодействует с роботом через REST интерфейс
- использует для авторизации уже известный ему уникальный PIN код (программная реализация механизма передачи PIN кода клиенту не требуется), но этот же PIN код использует и Fleet management service при отправке роботу задания на доставку

Fleet management service

- в задаче использует только REST интерфейс
- принимает параметры задачи от "сотрудника склада" (для простоты) - POST запросом из Postman или аналогичного инструмента
- принимает от Communication service уведомление о возвращении робота на склад и сохраняет в журнале (выводит на консоль)

Communication service

- получает параметры доставки по REST интерфейсу, отправляет их в шину сообщений
- получает уведомление о выполнении доставки и возвращении на базу из шины сообщений
- по REST интерфейсу уведомляет сервис управления парком роботов о прибытии

Central control unit

Центральный управляющий модуль (сервис)

- подписан на сообщения всех сервисов
- получает от communication service информацию о новой доставке, перепаковывает в сообщение с уменьшенным количеством информации (убирает PIN доступа) и публикует в своём топике

- получает информацию о текущем положении и рассчитывает параметры управления, которые публикует отдельном топике

в случае приближения к месту назначения даёт команду на остановку движения

- при получении информации об обнаружении объекта и вводе PIN код даёт команду на открытие хранилища
- после получения информации о закрытой крышке хранилища начинает движение обратно на склад
- получает информацию о координатах и рассчитывает управление
- при прибытии на склад останавливает движение

Positioning

- выдаёт текущие координаты (x, y) - удаление в метрах ("от центра города")
- использует параметры движения от сервиса motion control для вычисления изменения координат
- для простоты предположим, что препятствий нет и доставщик может ехать по прямой и поворачиваться (с ограничениями, см. motion control)

Motion control

- берёт на вход желаемые параметры направления и скорости движения
- применяет ограничения
  - скорость не более 5 км/ч
- по запросу способен выдать информацию об имеющихся физических ограничениях
- выдаёт параметры движения после применения ограничений

Sensors

- уведомляет об обнаружении объекта и его типе
  - Для простоты - берёт координаты и расстояние до цели, при приближении к цели меньше 10 см всегда обнаруживает объект типа "человек".
- управляет состоянием замка хранилища
  - при получении сообщения открывает замок
  - через фиксированное время (например, 5 сек) передаёт сообщение о закрытии замка

HMI

- имеет два интерфейса
  - с шиной сообщений
  - REST интерфейс для обработки запросов с PIN кодом
- при получении REST запроса с PIN отправляет сообщение в топик