

Опыт разработки требований в автомобильной индустрии: как учесть все стандарты и создать продукт



**Kaspersky
Automotive
Secure Gateway**

Олеся Васильева
Александра Крылова

kaspersky

Олеся Васильева

System Analyst Team Lead
kaspersky



Olesya.Vasilyeva@kaspersky.com
tg @olesia

План доклада

Что такое автомобильный шлюз KASG

Источники требований для KASG

Схема управления требованиями AS IT WAS

Схема управления требованиями AS IS

Заключение

План доклада

Что такое автомобильный шлюз KASG

Источники требований для KASG

Схема управления требованиями AS IT WAS

Схема управления требованиями AS IS

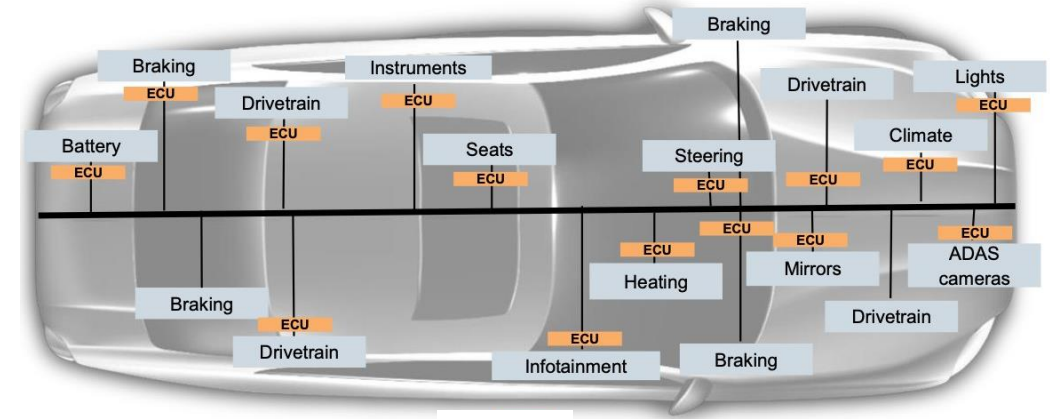
Заключение

Что такое автомобильный шлюз KASG

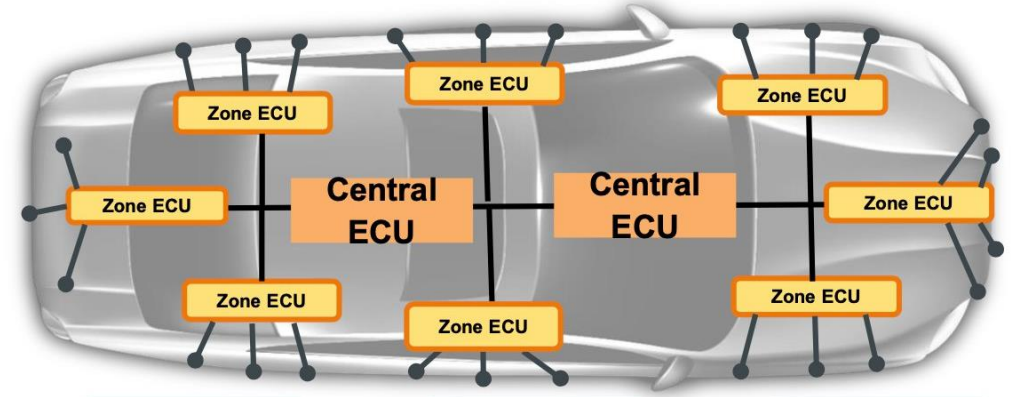
Эволюция E/E-архитектуры автомобилей



Распределенная архитектура с множеством простых ЭБУ



Функции ЭБУ консолидированы по зонам/доменам



Что такое автомобильный шлюз KASG

Угрозы в индустрии

С 2018 по 2023:

225% рост количества
подключенных автомобилей

134% рост
кибератак

В современных автомобилях функциональная безопасность и кибербезопасность – одно и то же

Дэн Амманн (2018, ex- President GM)

Источник: Juniper Research, Upstream Security Ltd.

Что такое автомобильный шлюз KASG

Рейтинг атак

до **\$1,1 млрд**

может стоить автопроизводителю
одна кибератака

26%



Системы бесключевого
доступа

40%



Облачная
и серверная
инфраструктура

12%



Телематический
блок и центральный
шлюз

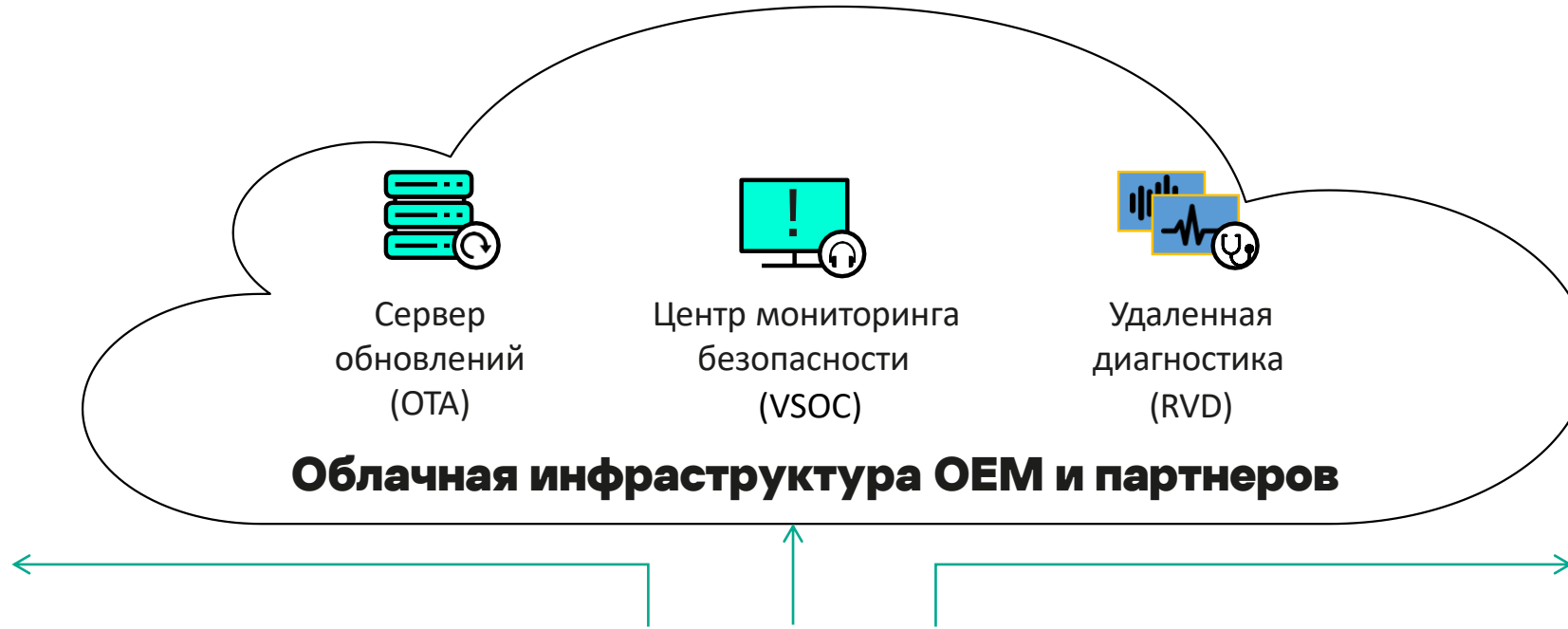
Автомобильный шлюз безопасности Kaspersky Automotive Secure Gateway



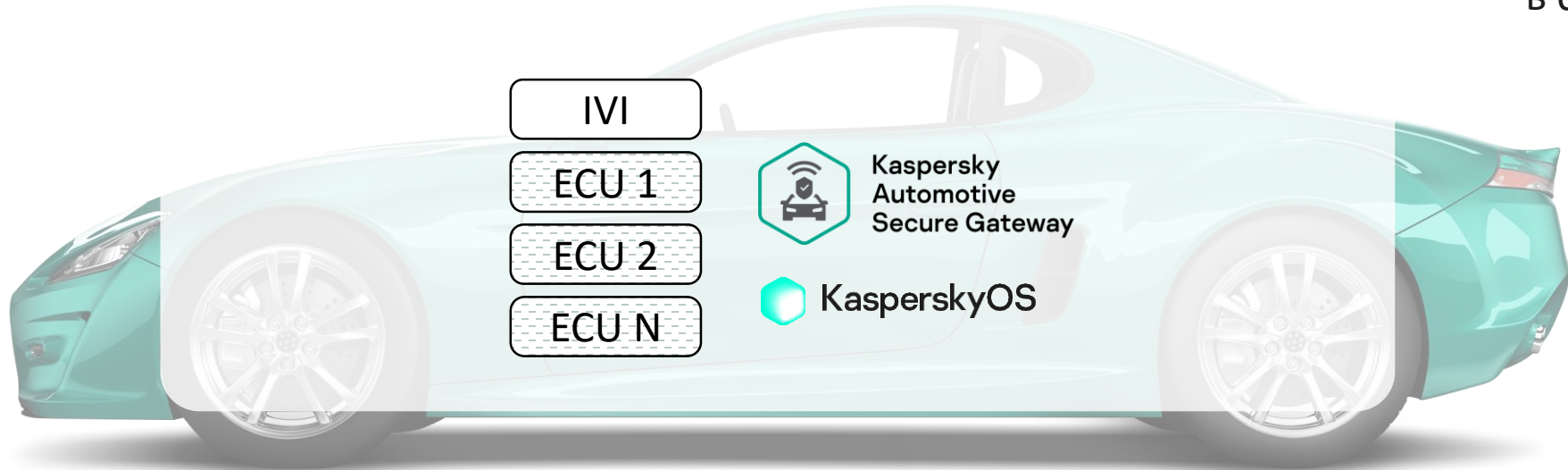
Kaspersky Automotive Secure Gateway



Смартфоны водителя и пассажиров



Устройства диагностики в сервис-центрах



План доклада

Что такое автомобильный шлюз KASG

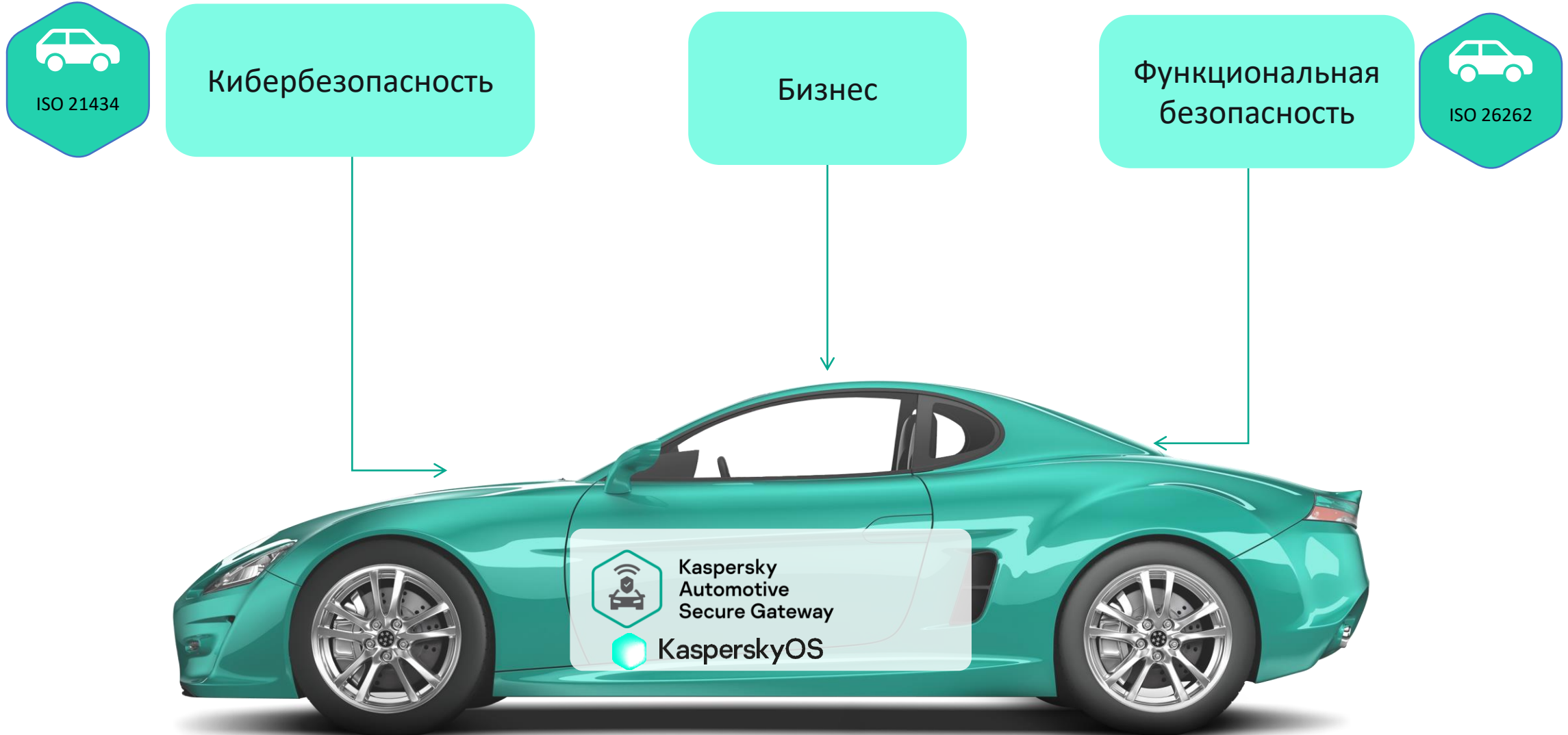
Источники требований для KASG

Схема управления требованиями AS IT WAS

Схема управления требованиями AS IS

Заключение

Источники требований для KASG



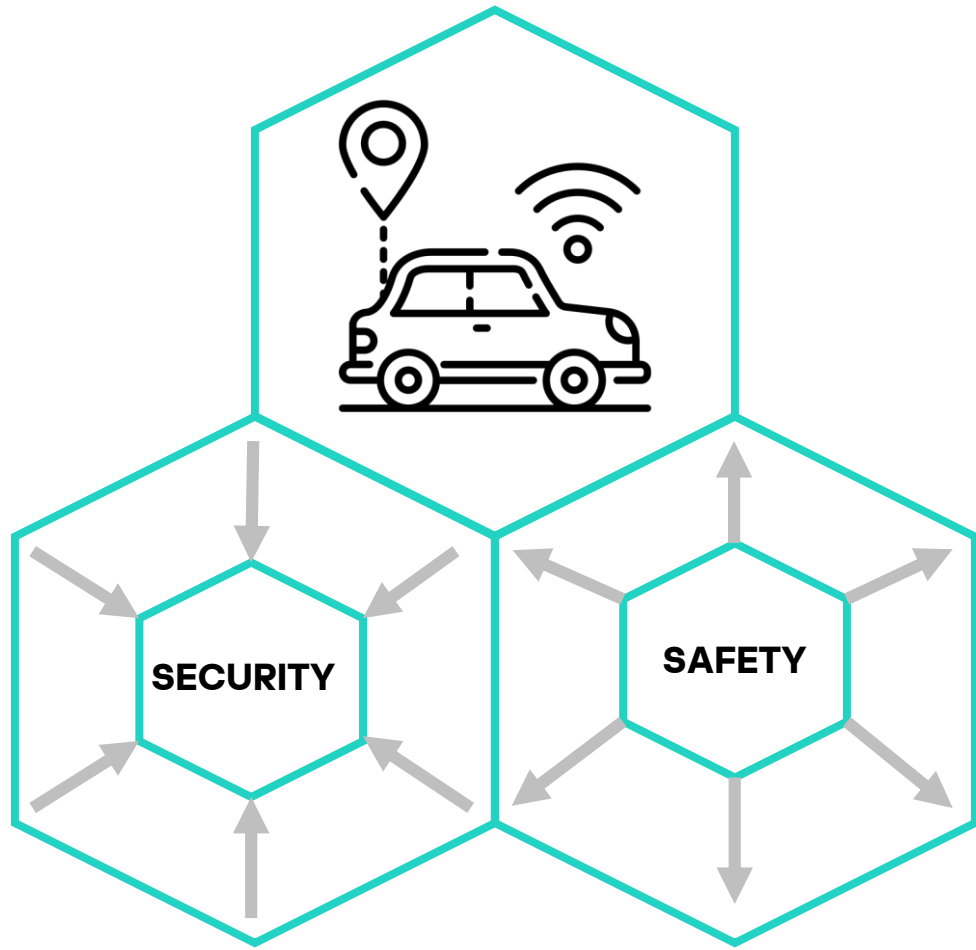
Источники требований для KASG



Источники требований для KASG



Источники требований для KASG



Александра Крылова

Senior System Analyst
kaspersky



Aleksandra.Krylova@Kaspersky.com
tg @AleksKrylova

История разработчика из банковского сектора на автомобильном проекте в роли аналитика..

План доклада

Что такое автомобильный шлюз KASG

Источники требований для KASG

Схема управления требованиями AS IT
WAS

Схема управления требованиями AS IS

Заключение

Схема управления требованиями

Как было и почему не эффективно

Специалисты на проекте – аналитики по функциональной и кибер- безопасности

Параллельные стримы

Как стало, оптимизация

Разделение системных требований на уровни

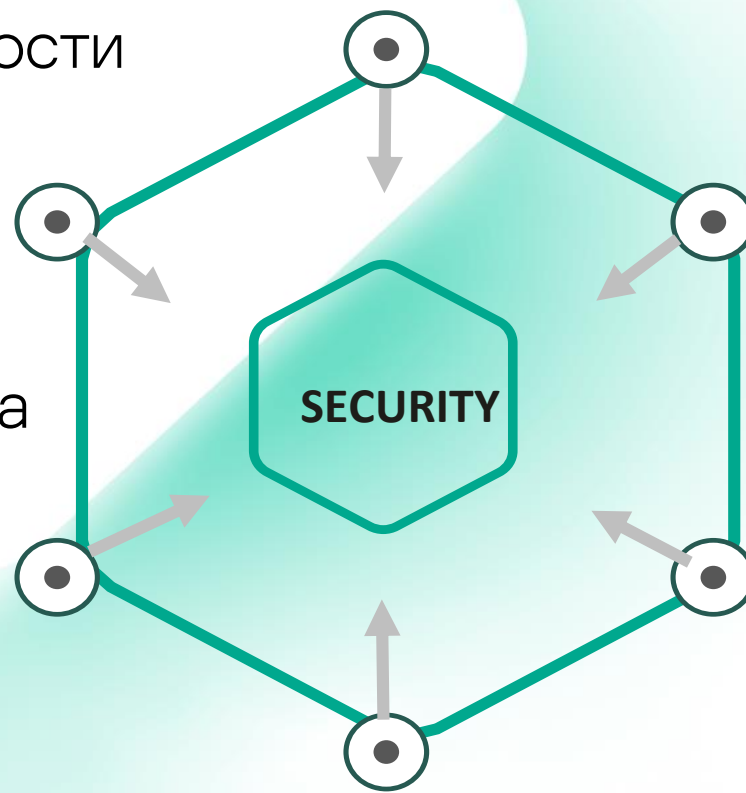
Трассировка требований

Процесс управления требованиями

Security Champion

Эксперт по кибербезопасности

Окр. среда -> система



Проводит TARA – анализ

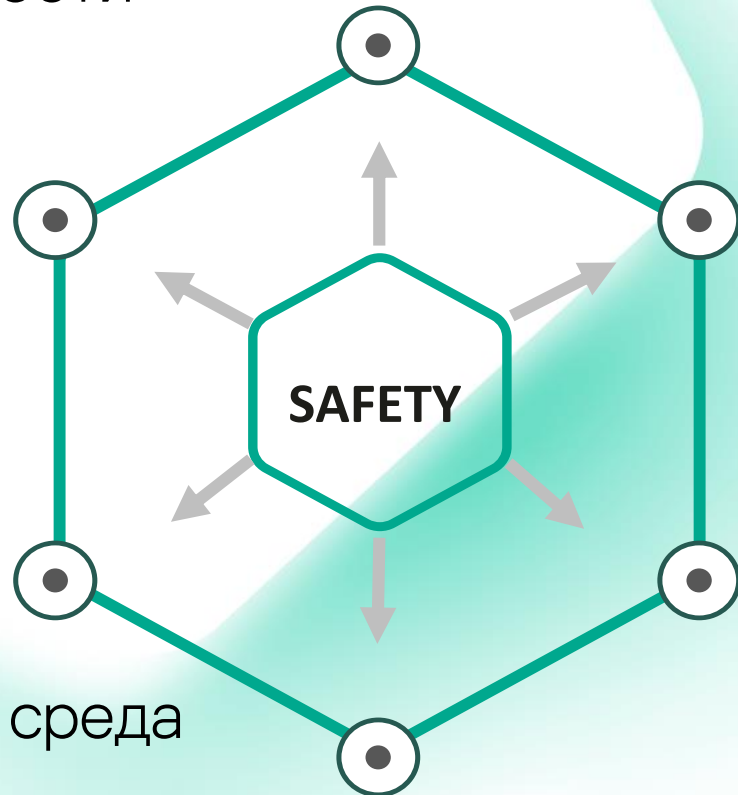
Выполняет оценку влияния бизнес функционала на кибербезопасность

Разрабатывает концепции безопасности

Отвечает за создание киберимунной архитектуры

Safety Engineer

Инженер по
функциональной
безопасности

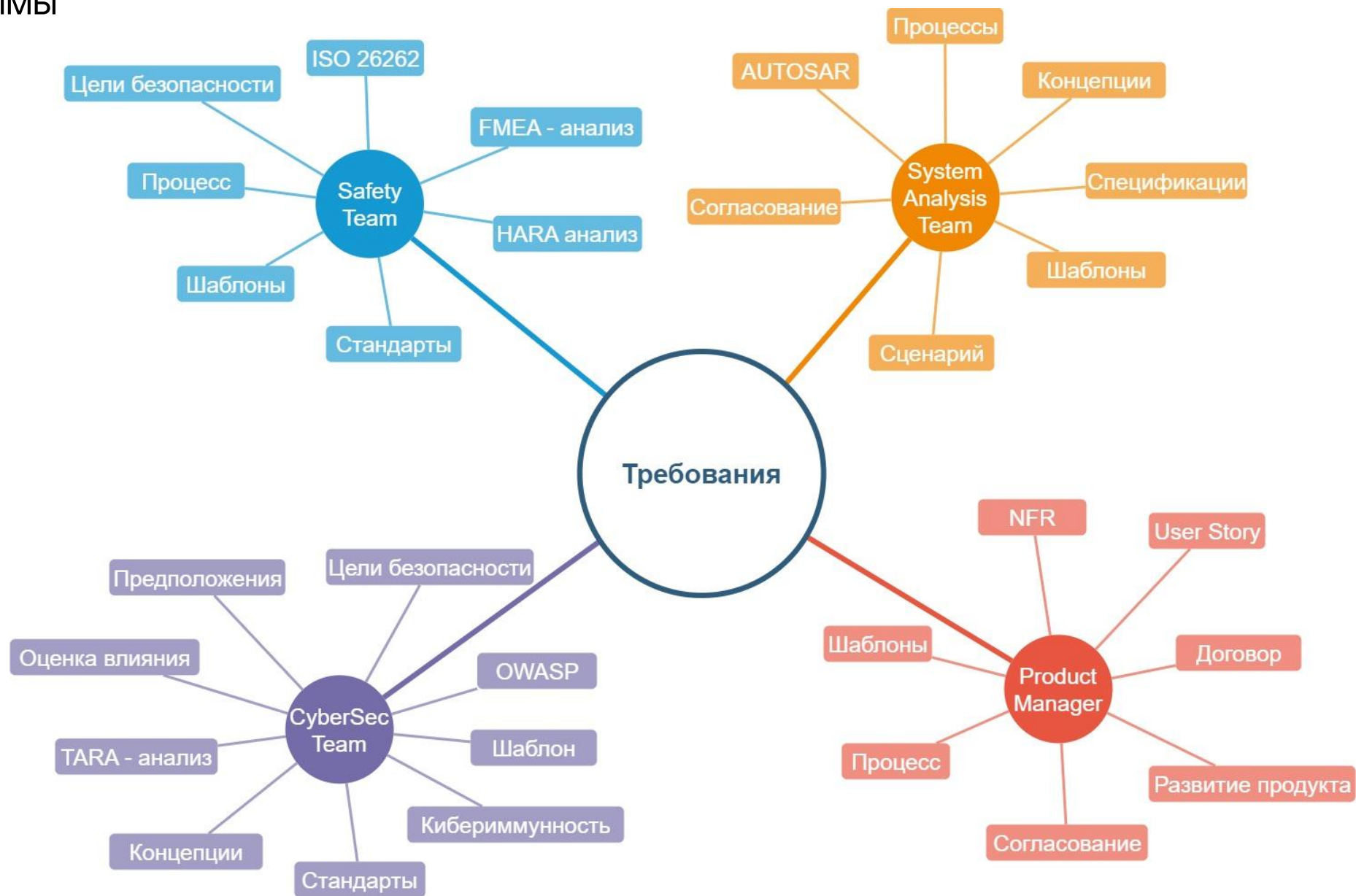


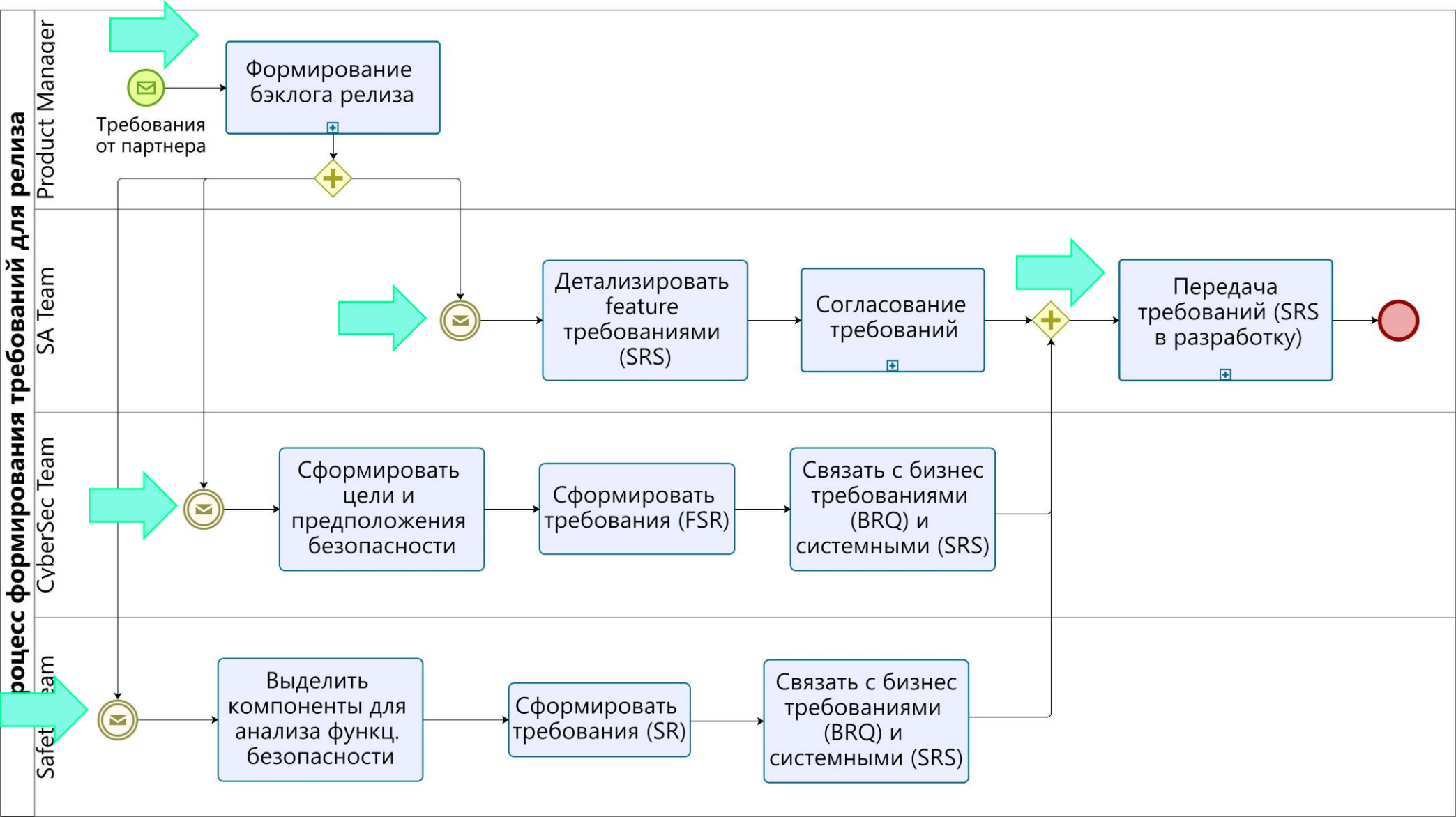
Определяет уровень полноты
безопасности

Определяет цели безопасности

Проводит анализы
Безопасности (HARA)

Формирует требования
функциональной безопасности





Почему не эффективно?

Риск потери критичных функций
в реализации функционала

В результате анализов –
разные типы требований

Пересечение функциональности
и отсутствие трассировки

Несогласованность работ

План доклада

Что такое автомобильный шлюз KASG

Источники требований для KASG

Схема управления требованиями AS IT
WAS

Схема управления требованиями AS IS

Заключение

Схема управления требованиями

Как было и почему не эффективно

Специалисты на проекте – аналитики по функциональной и кибер- безопасности

Параллельные стримы

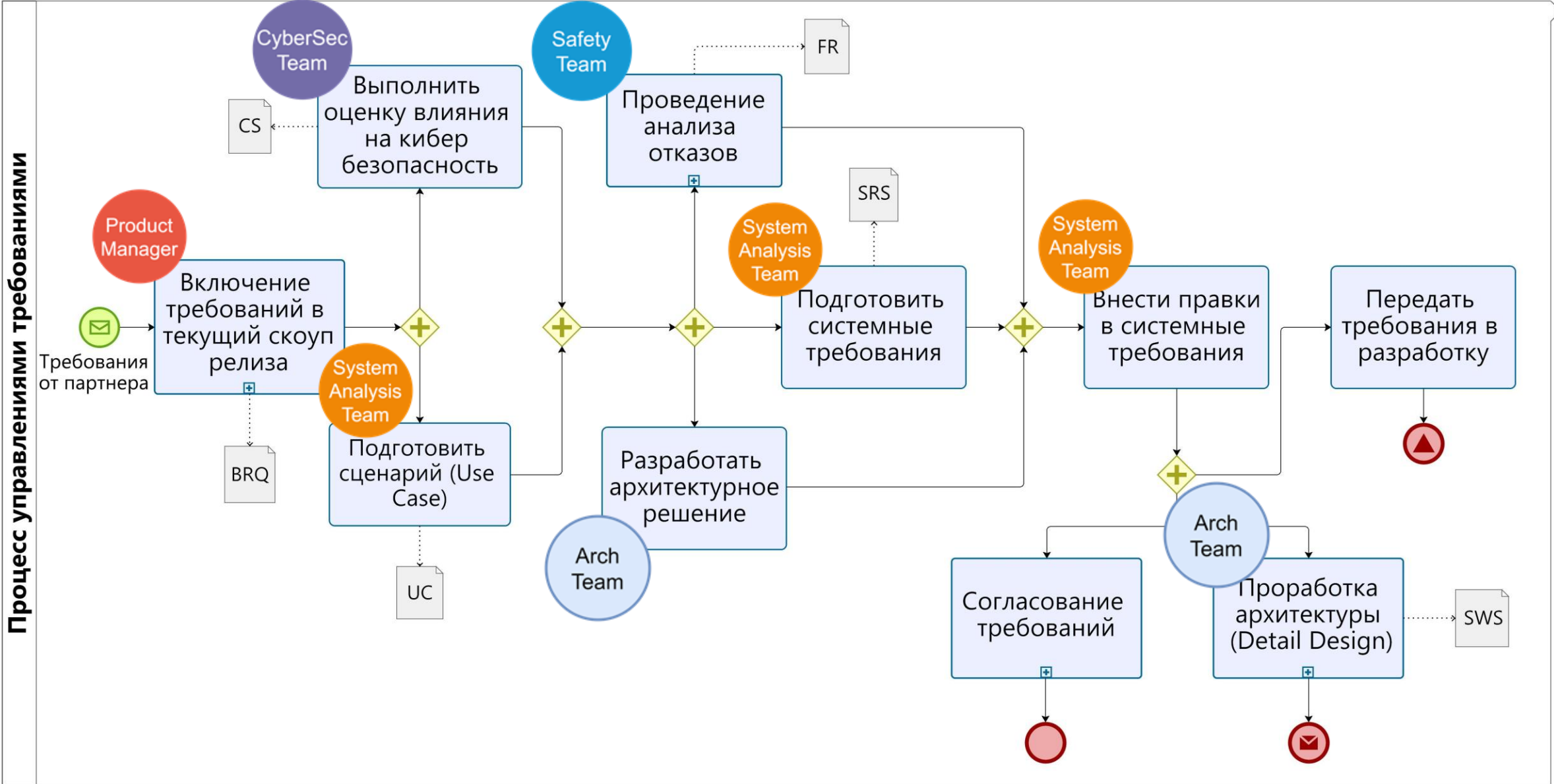
Как стало, оптимизация

Классификация требований

Процесс управления требованиями

Трассировка требований





Почему было не эффективно?

Риск потери критичных функций
в реализации функционала

В результате анализов –
разные типы требований

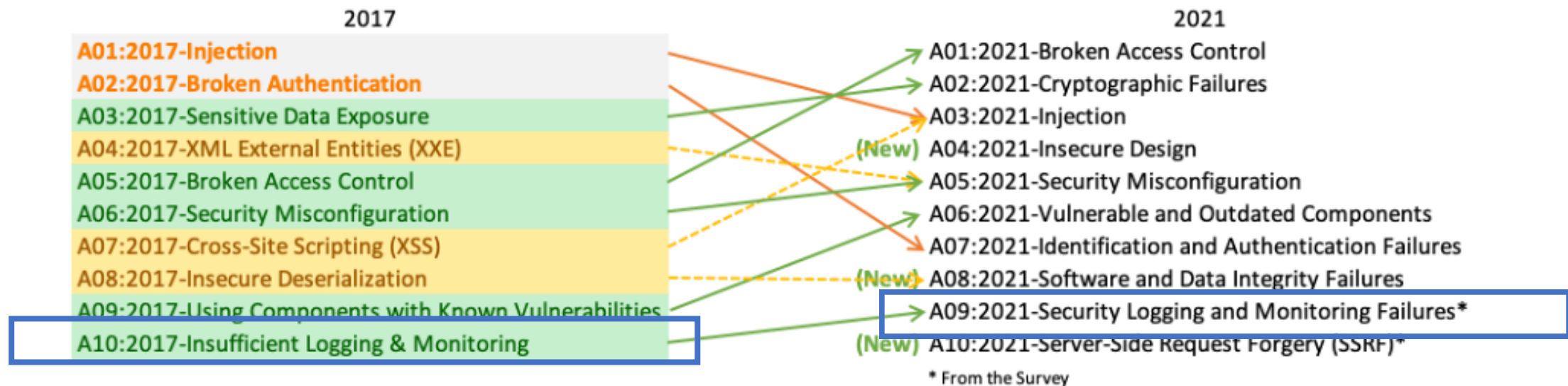
Пересечение функциональности
и отсутствие трассировки

Несогласованность работ

The OWASP Top 10

регулярно-обновляемый отчет*, содержащий описание проблем безопасности веб-приложений с упором на 10 наиболее критичных рисков.

*Отчет составляется командой экспертов по безопасности со всего мира.



Риск потери критичных функций

Сбои в безопасности журналирования и мониторинга

A09:2021-Security Logging and Monitoring Failures

Недостаточность ведения журналов

Отказ системы из-за переполнения хранилища

Включение конфиденциальной информации в журнал

Система логирования выполняет зловредный код

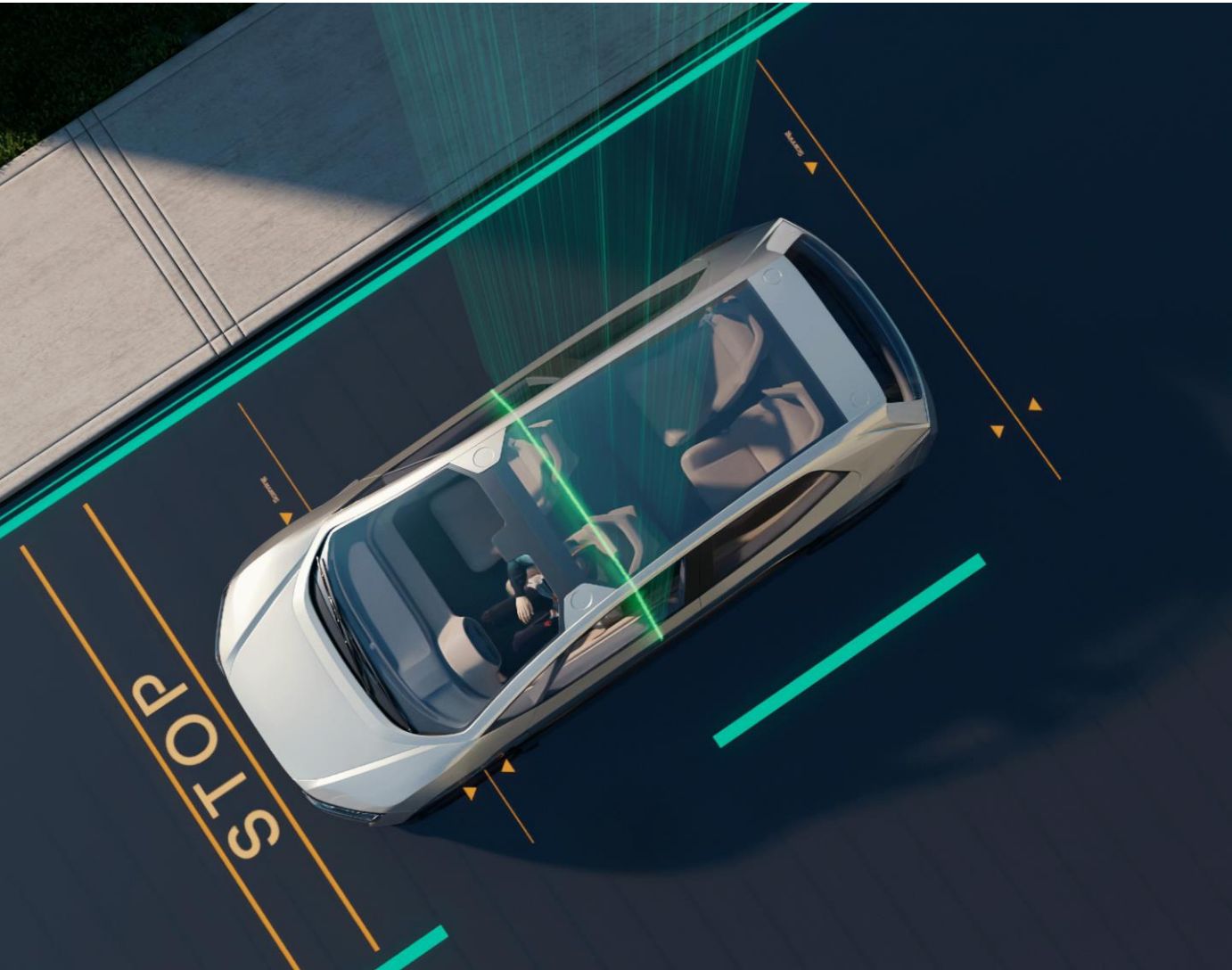
Риск потери критичных функций

Гарантия доставки сообщений в сценарии удаленной парковки

Резервирование каналов передачи данных

Использование механизмов безопасности сообщений

Оптимизация



Согласованная работа команд аналитиков

Понятный процесс управления требованиями

Трассировка требований и минимизация риска потери важного функционала

Заключение



Опыт полезен всем, кто сталкивается с разными стандартами, не только в автомобилях

Спасибо!

Олеся Васильева

Olesya.Vasilyeva@kaspersky.com

tg @olesia

Александра Крылова

Aleksandra.Krylova@Kaspersky.com

tg @AleksKrylova

kaspersky