CODESYS ПЛК на базе Kaspersky OS

BE. services

Ключевые проблемы безопасности и их причины

Уязвимости

- ✓ Человеческие ошибки
- ✓ Использование стороннего программного обеспечения
- ✓ Сложность программного обеспечения

Небезопасный дизайн ПО

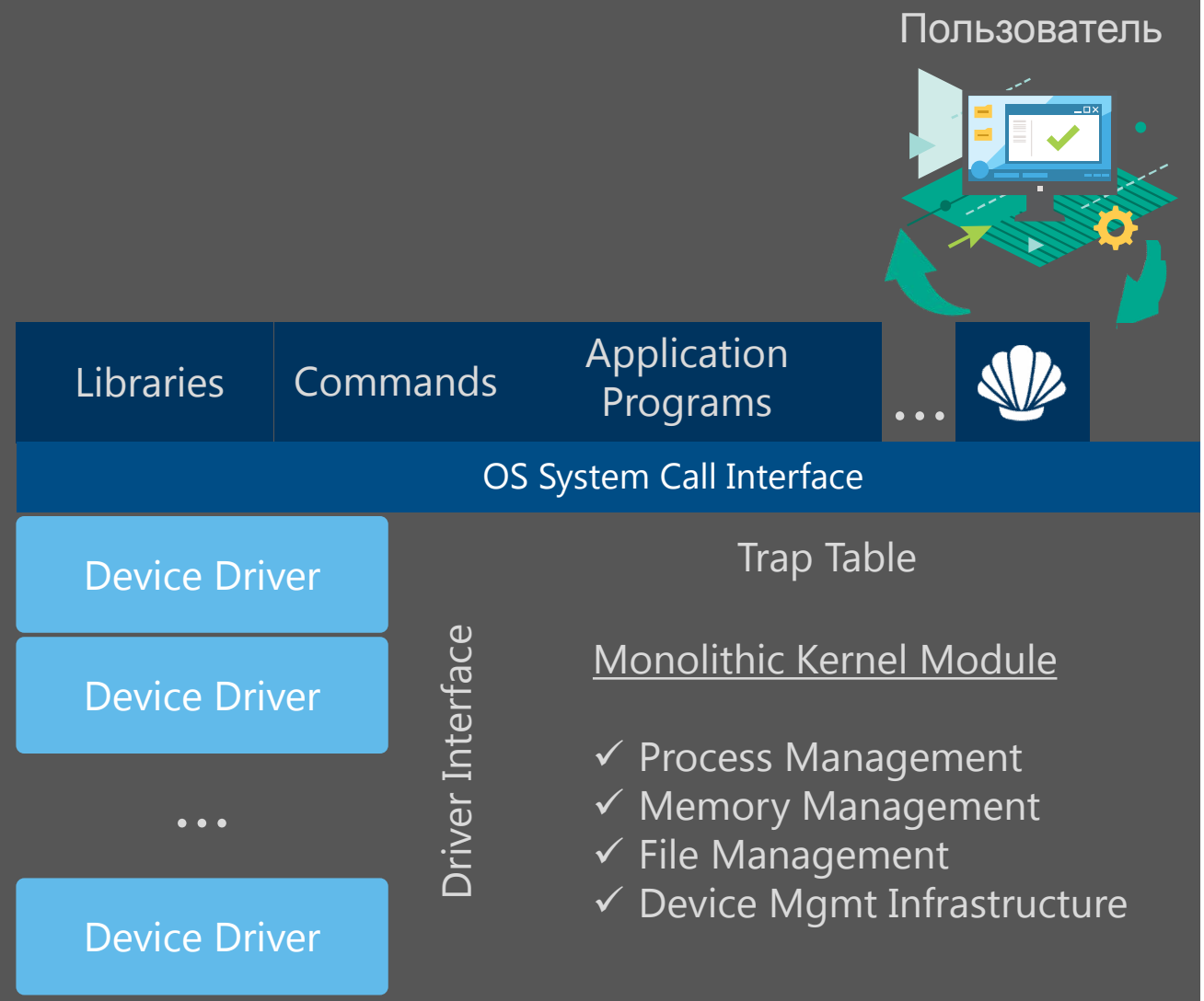
- ✓ Время выпуска продукции имеет приоритет

Использование традиционных ОС

© BE.services GmbH

Почему традиционные ОС небезопасны?

- Монолитная архитектура, где модули могут вызывать друг друга
- При обнаружение уязвимости можно вызвать код любого модуля
- Неконтролируемые библиотеки сторонних производителей
- Используя одну уязвимость, можно получить доступ ко всей системе
- Недостаточные настройки безопасности
- Большая поверхность атак



© BE.services GmbH

KasperskyOS: История

© BE.services GmbH

ДВЕ ИДЕИ

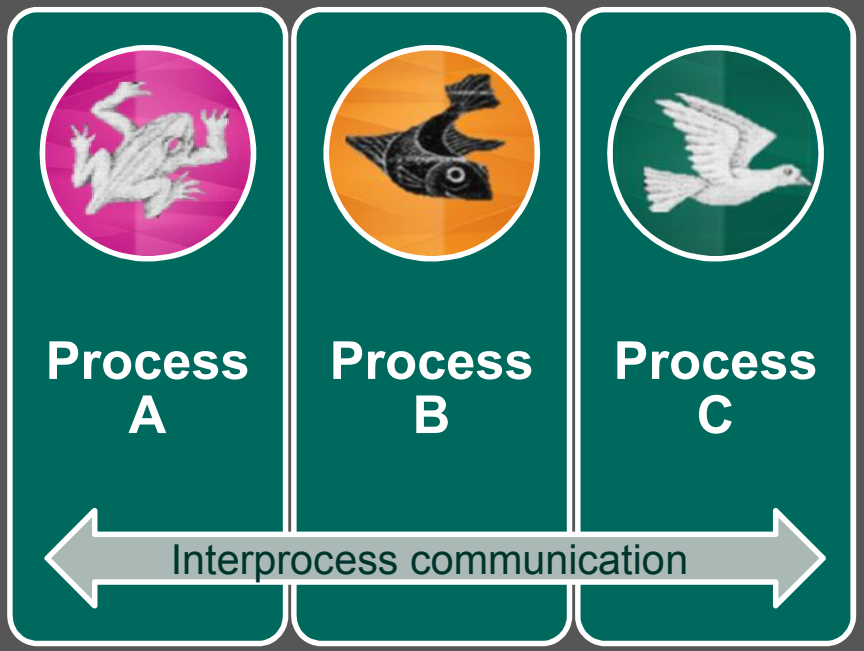
Микроядерная архитектура для разделения доменов безопасности

+

Выделенная система безопасности для регулирования взаимодействия доменов

© BE.services GmbH

ИДЕЯ НОМЕР 1

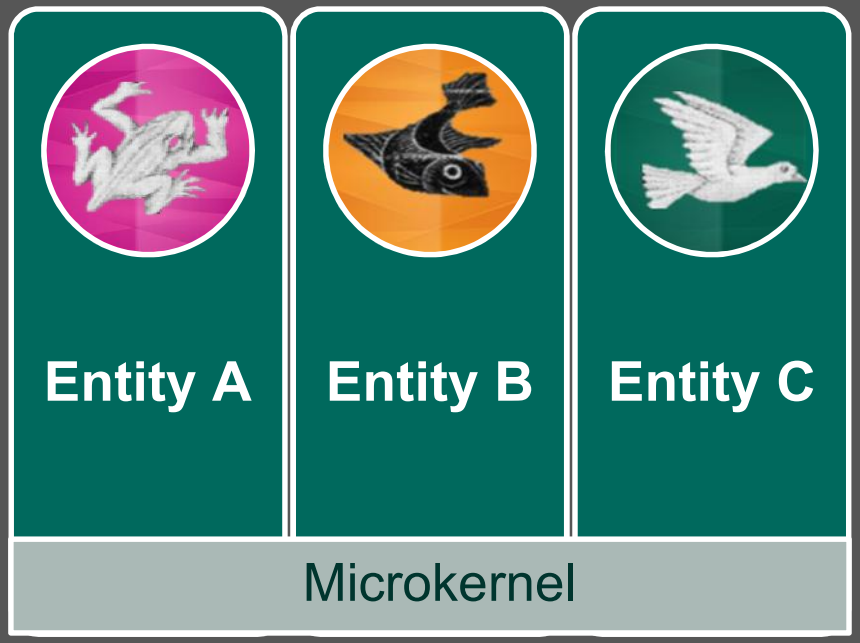


Единый механизм связи между процессами (IPC)

- Реализуется с помощью микроядра
- Обеспечение полного контроля

© BE.services GmbH

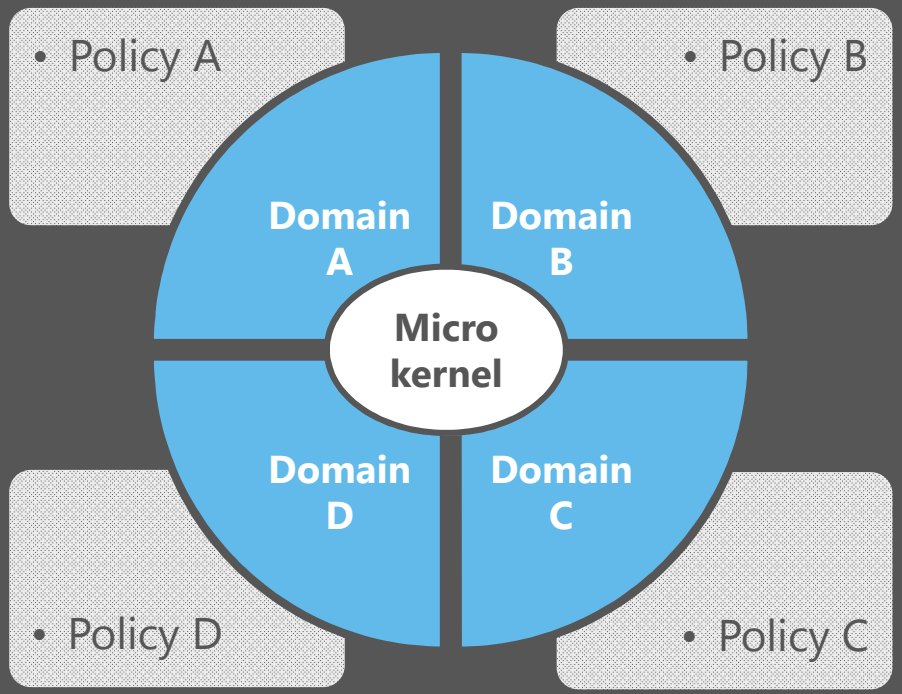
МИКРОЯДРО



- Микроядро реализует IPC
- Нет никакого другого способа связи в системе, кроме IPC
- Связь асинхронная

© BE.services GmbH

РАЗДЕЛЯЮЩЕЕ ЯДРО



Задача разделяющего ядра – это создание системы, которая не отличается от системы разделенной физически

© BE.services GmbH

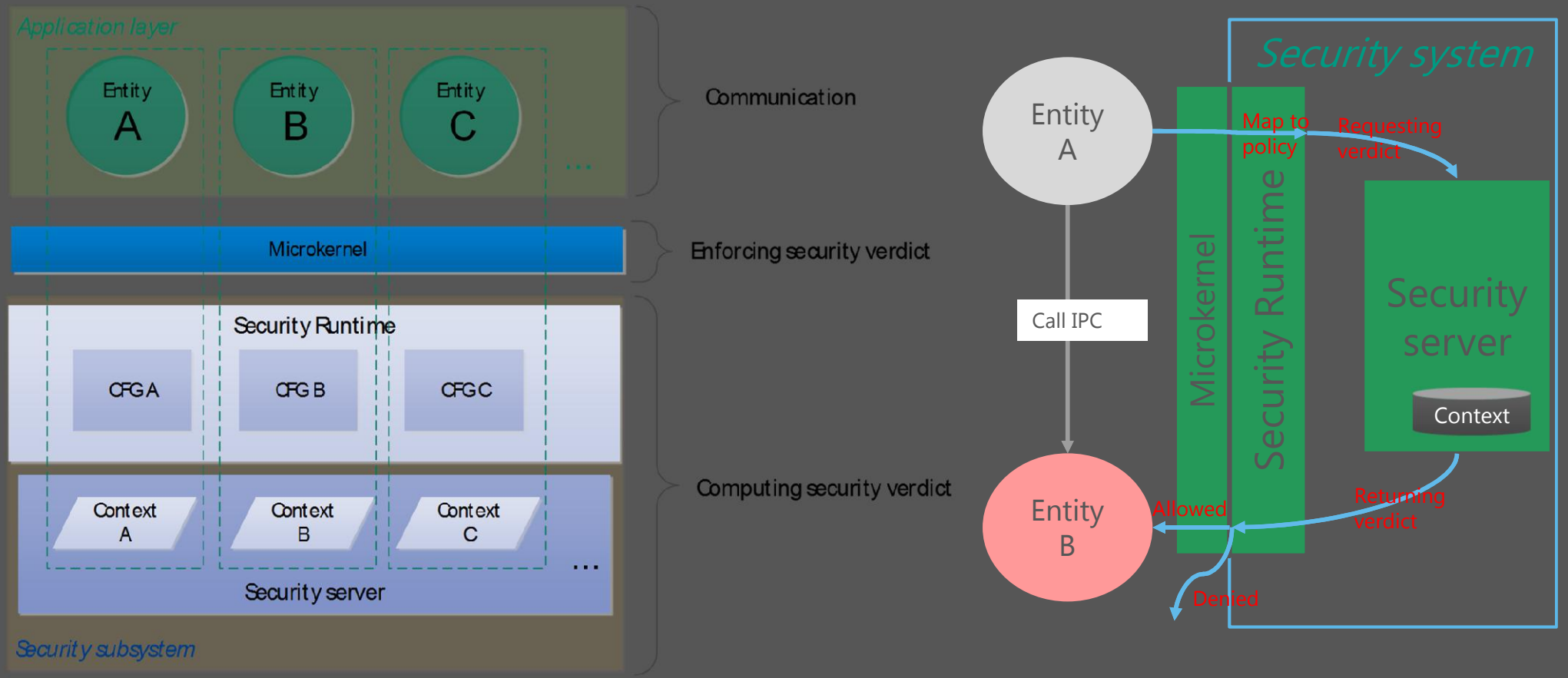
ИДЕЯ НОМЕР 2

Отдельная система безопасности

Гибкое управление всеми связями в системе

© BE.services GmbH

Дизайн архитектуры в KasperskyOS



© BE.services GmbH

Языки конфигурирования

Для описания доменов безопасности и их взаимодействий

- IDL - Interface Definition Language
- CDL - Component Definition Language
- EDL - Entity Definition Language

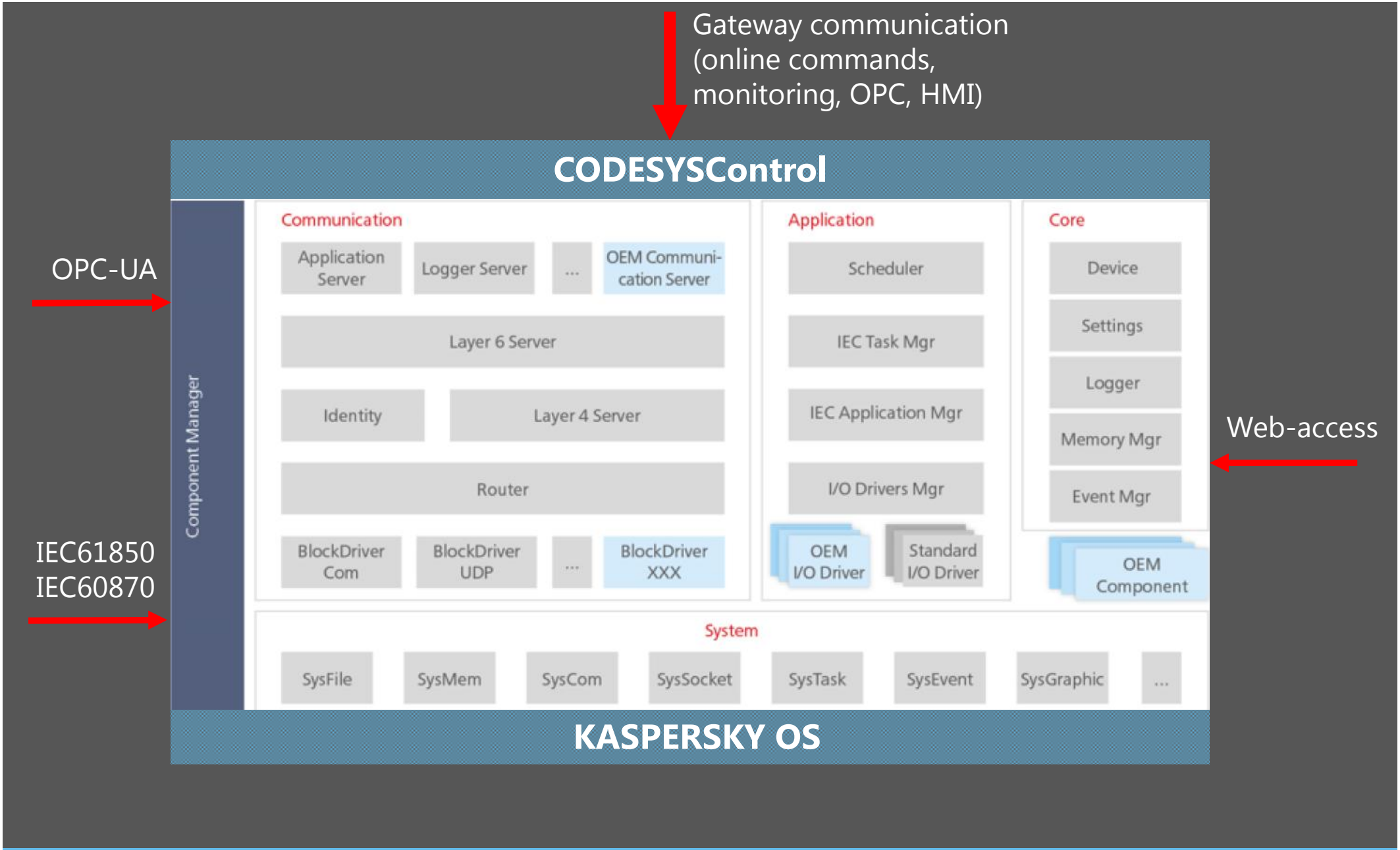
© BE.services GmbH

Дополнительные функции безопасности

- Безопасная загрузка (secure boot)
- Безопасный аудит (secure audit)
- Безопасное хранилище данных (secure storage)
- Безопасный канал связи (trusted channel)
- Безопасное обновление программного обеспечения (secure update)

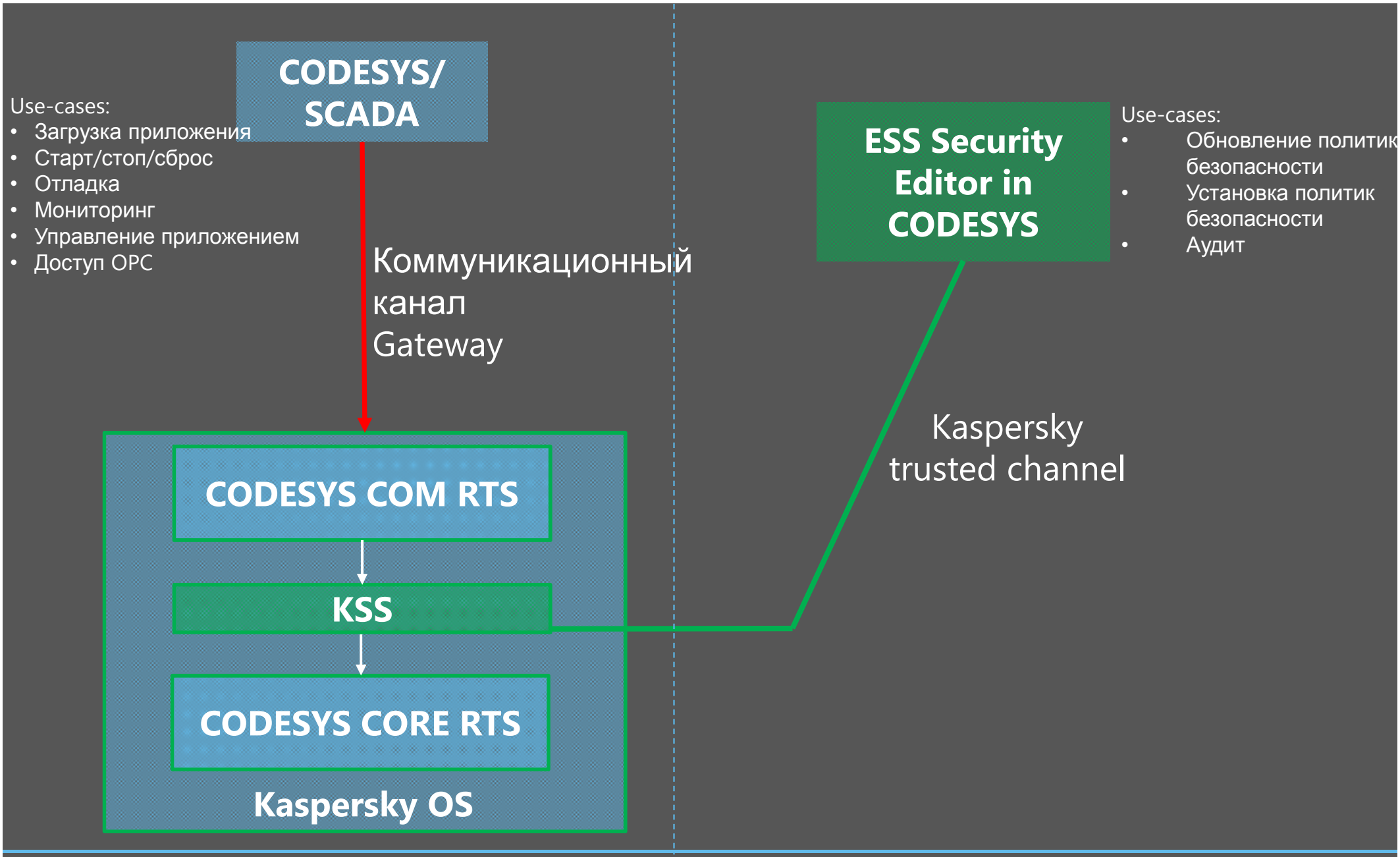
© BE.services GmbH

Архитектура CODESYSControl в KOS



© BE.services GmbH

Embedded Security Shield (ESS) в KOS



© BE.services GmbH

Заключение

- ПЛК работает под управлением безопасной операционной системы, которая содержит только необходимый программный код. Благодаря этому вероятность наличия уязвимости мала (маленькая поверхность атак)
- Интеграция с ESS
- Безопасность – это парадигма разработки ПЛК
- Наличие дополнительных надежных функций безопасности
- Возможные проблемы безопасности в интегрированном программном обеспечен не являются проблемами безопасности системы в целом

© BE.services GmbH

Thank you very much for your attention!

Copyright © 2018 by BE.services GmbH.
All rights reserved. This document or any portion thereof may not be reproduced, distributed or transmitted in any form or by any means including photocopying, recording, or other electronic methods, without the prior written permission of BE.services GmbH.