Мониторинг состояний системы, построенной на основе адаптивной MILS платформы

Екатерина Рудина

Лаборатория Касперского

KASPERSKY lab

Содержание

Эволюция MILS платформы*

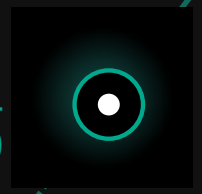
Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности

1980-2000



Идея Ядра Разделения как основы безопасной системы
В силу проблем с реализацией отложено

* Даты указаны приблизительно

MILS – Multiple Independent Levels of Security and Safety

MILS это архитектура системы, построенной с использованием ядра разделения (Separation Kernel, J.Rushby, “Design and Verification of Secure Systems”, SOSP ’81)

Информационная безопасность

1. Изоляция от недоверенного субъекта/кода/окружения, изоляция недоверенного субъекта/кода/окружения
2. Политики мандатного контроля доступа, разделение обязанностей
3. Раздельная валидация и верификация

Функциональная безопасность

1. Обеспечение невлияния
2. Раздельная верификация
3. Поддержка приложений с разными требованиями к реалтаймовому исполнению

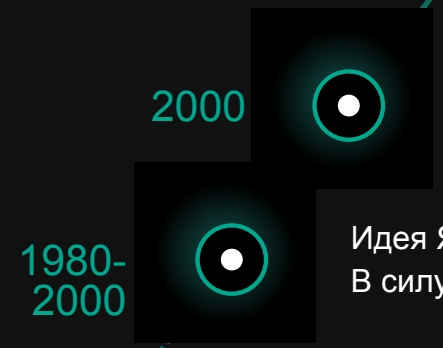
Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности



1980-2000

Идея Ядра Разделения как основы безопасной системы
В силу проблем с реализацией отложено

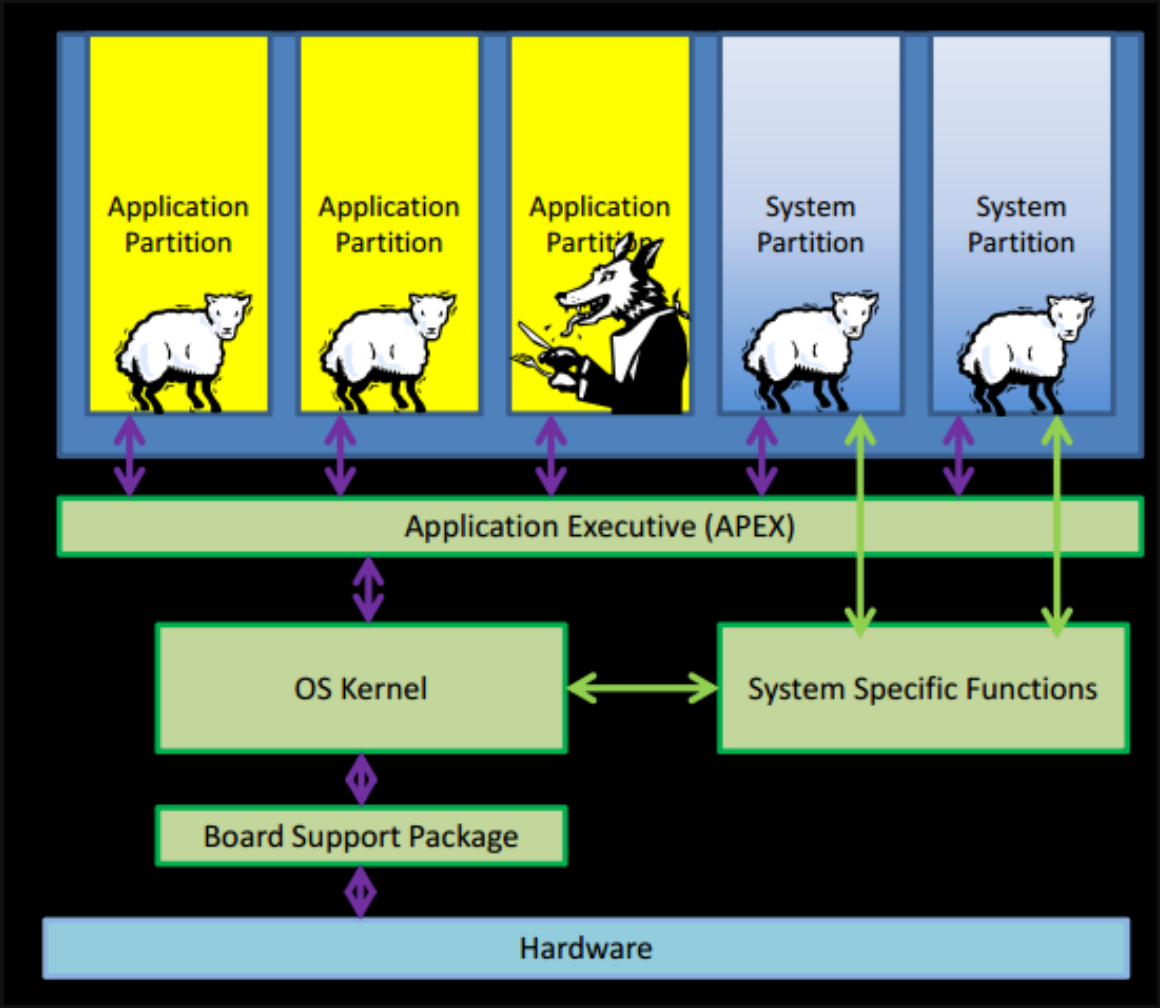
2000

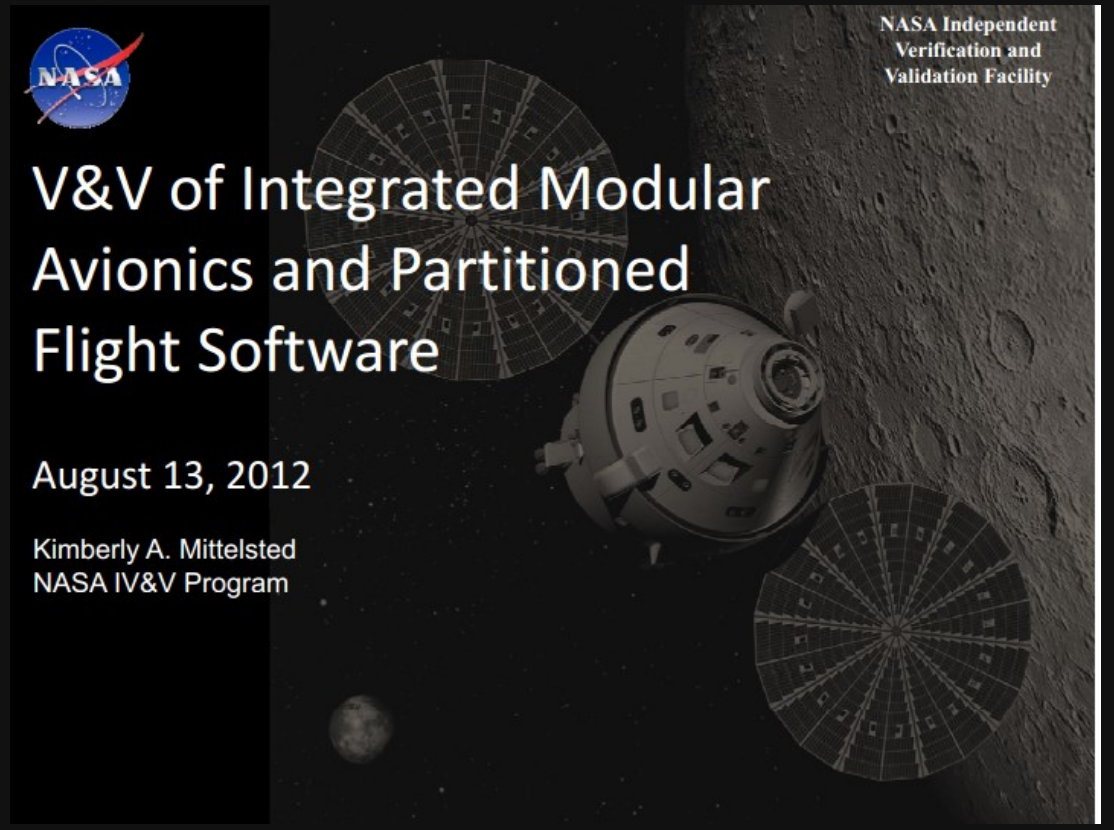
Исследование ядер коммерческих систем авионики для обеспечения информационной безопасности

* Даты указаны приблизительно

KASPERSKY lab

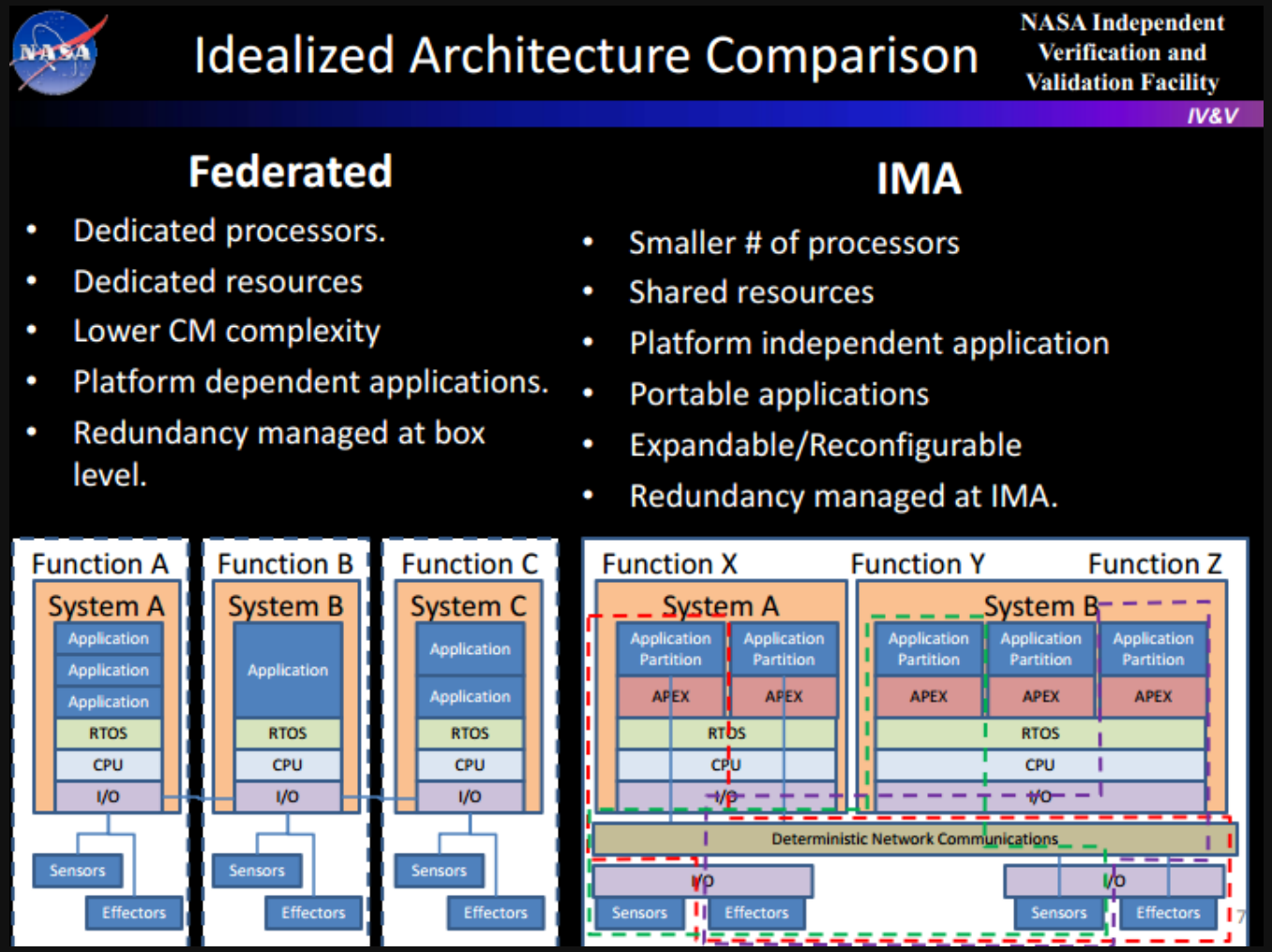
Другой источник





Источник: https://www.nasa.gov/sites/default/files/3-5b-2012_workshop_presentation_on_arinc_653_20120822_submitted_pdf.pdf

Ожидания - реальность



Источник: https://www.nasa.gov/sites/default/files/3-5b-2012_workshop_presentation_on_arinc_653_20120822_submitted_pdf.pdf

Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности

2004 — Развитие идей MILS, появление MILS community

2000 — Исследование ядер коммерческих систем авионики для обеспечения информационной безопасности

1980-2000 — Идея Ядра Разделения как основы безопасной системы
В силу проблем с реализацией отложено

* Даты указаны приблизительно

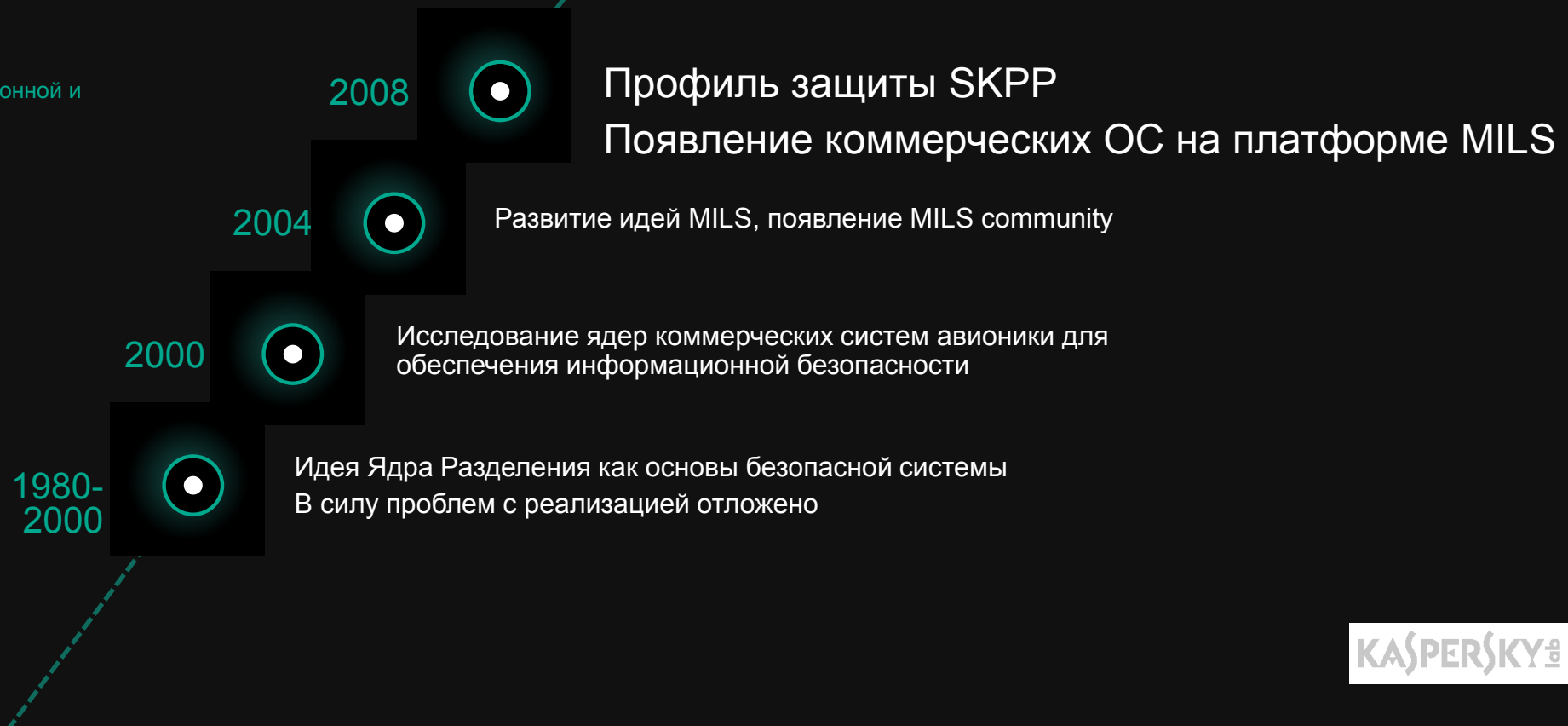
Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности



* Даты указаны приблизительно

KASPERSKY lab

Система, построенная на основе платформы MILS

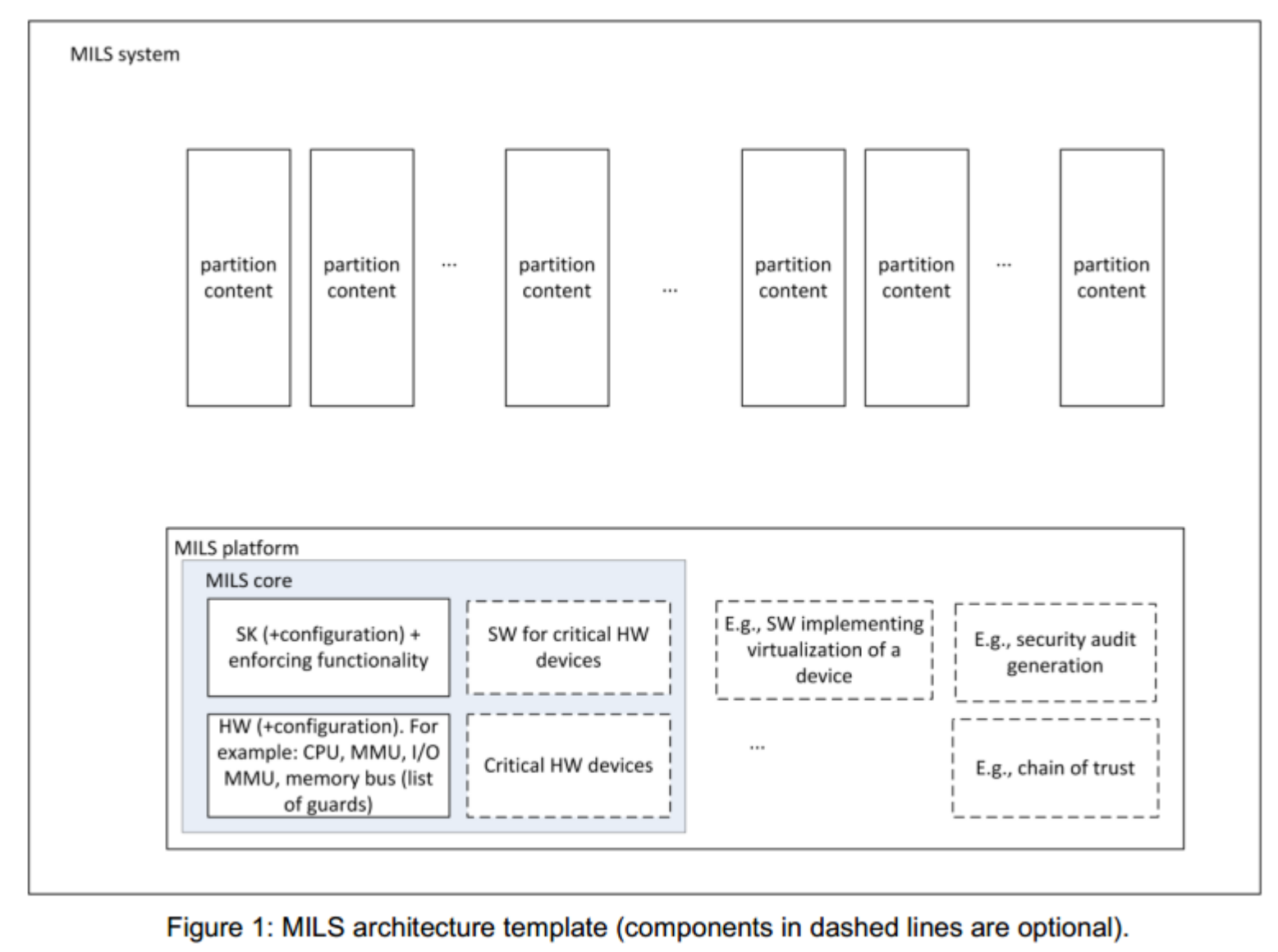


Figure 1: MILS architecture template (components in dashed lines are optional).

Источник: EUROMILS. MILS Architecture Whitepaper

Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности

2012 — Прототипирование динамического MILS и распределенной платформы MILS

2008 — Профиль защиты SKPP
Появление коммерческих ОС на платформе MILS

2004 — Развитие идей MILS, появление MILS community

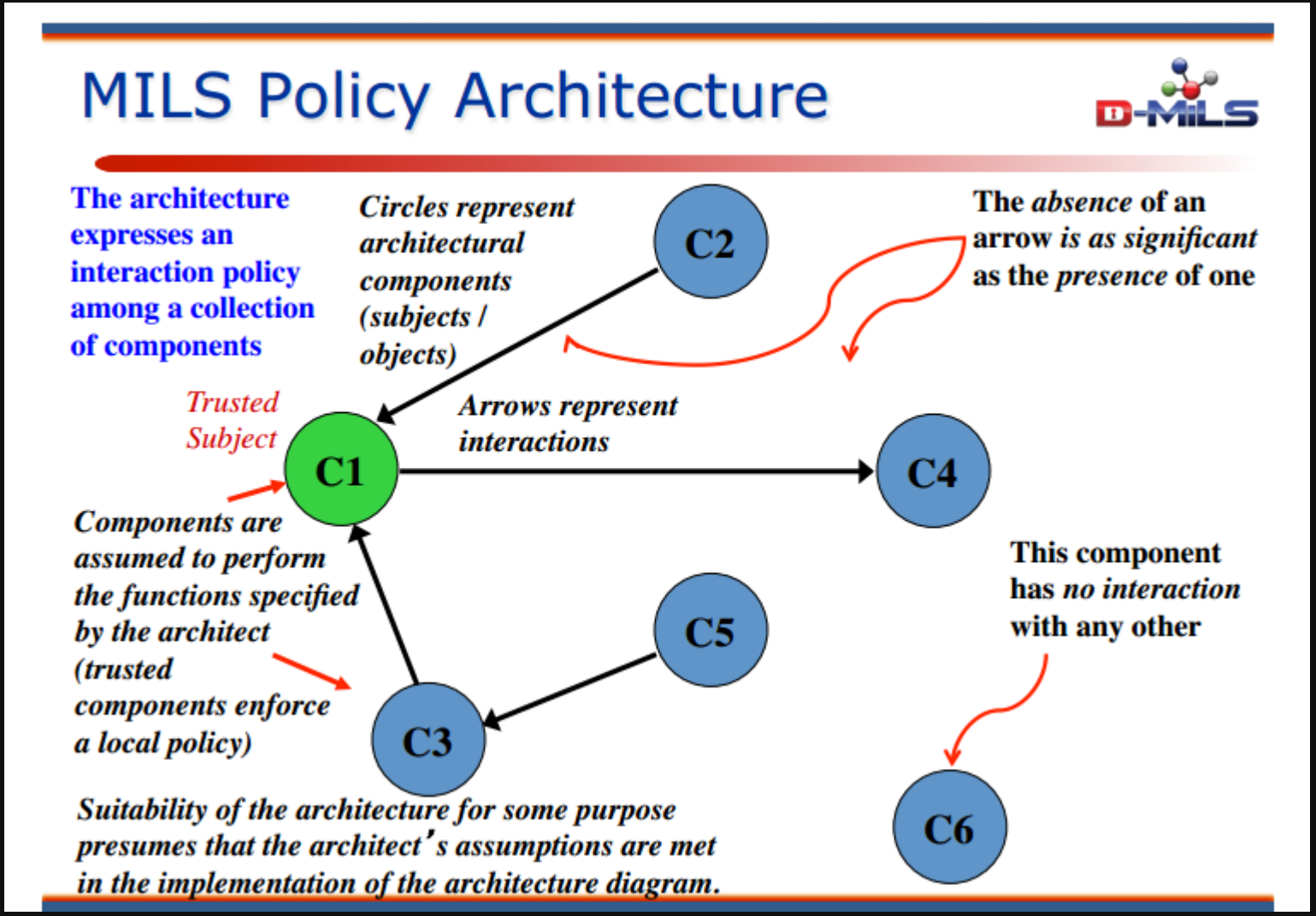
2000 — Исследование ядер коммерческих систем авионики для обеспечения информационной безопасности

1980-2000 — Идея Ядра Разделения как основы безопасной системы
В силу проблем с реализацией отложено

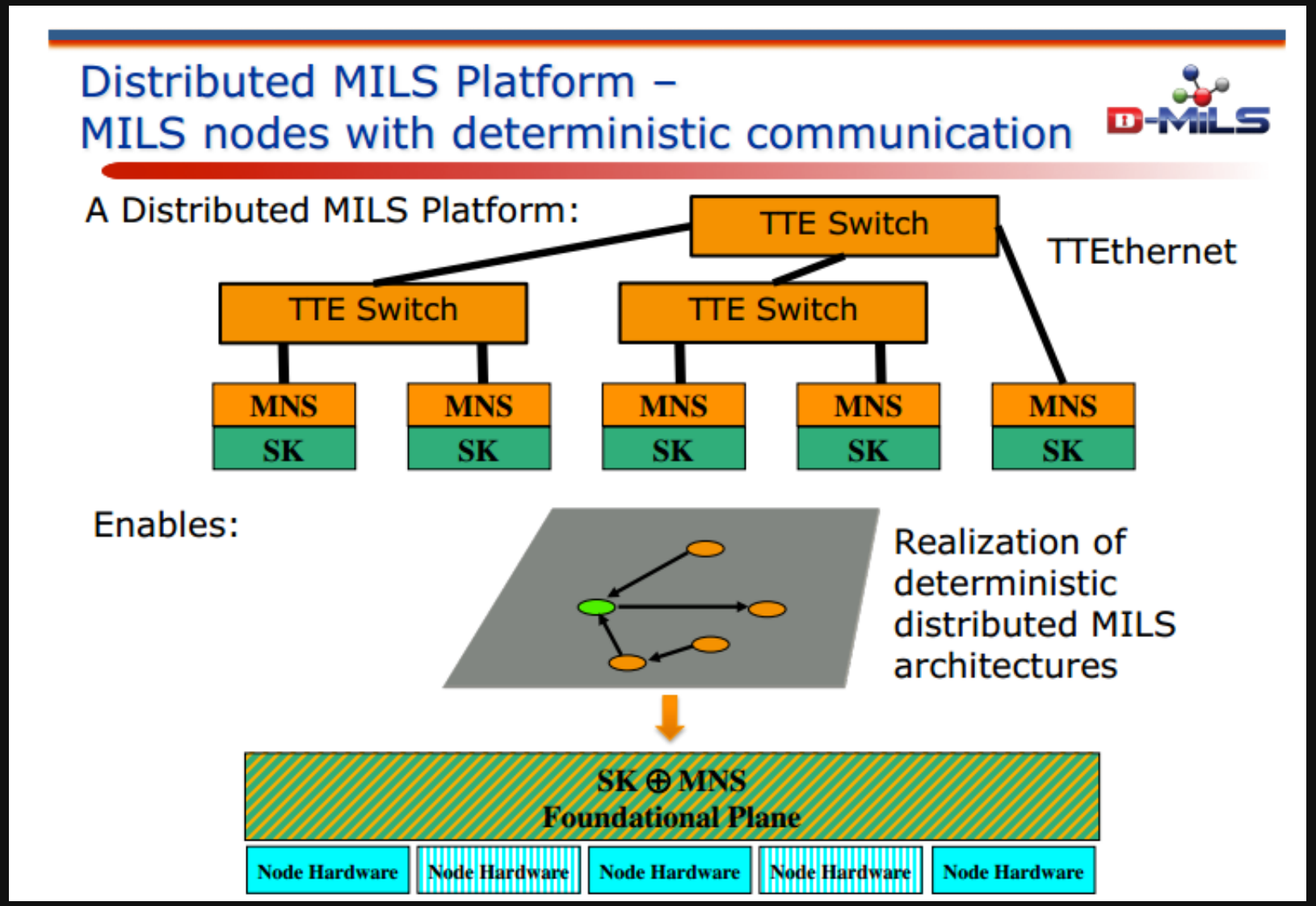
* Даты указаны приблизительно

KASPERSKY lab

MILS платформа: архитектура доверия



Распределенная MILS платформа



Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности

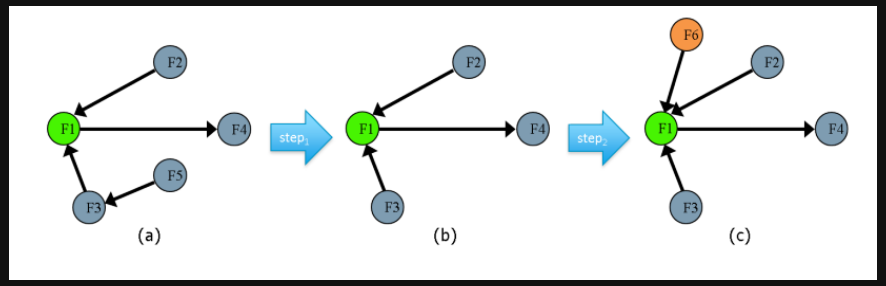
* Даты указаны приблизительно

Динамический MILS и Адаптивная MILS платформа для обеспечения устойчивости критической инфраструктуры

Критические инфраструктуры нуждаются в устойчивости

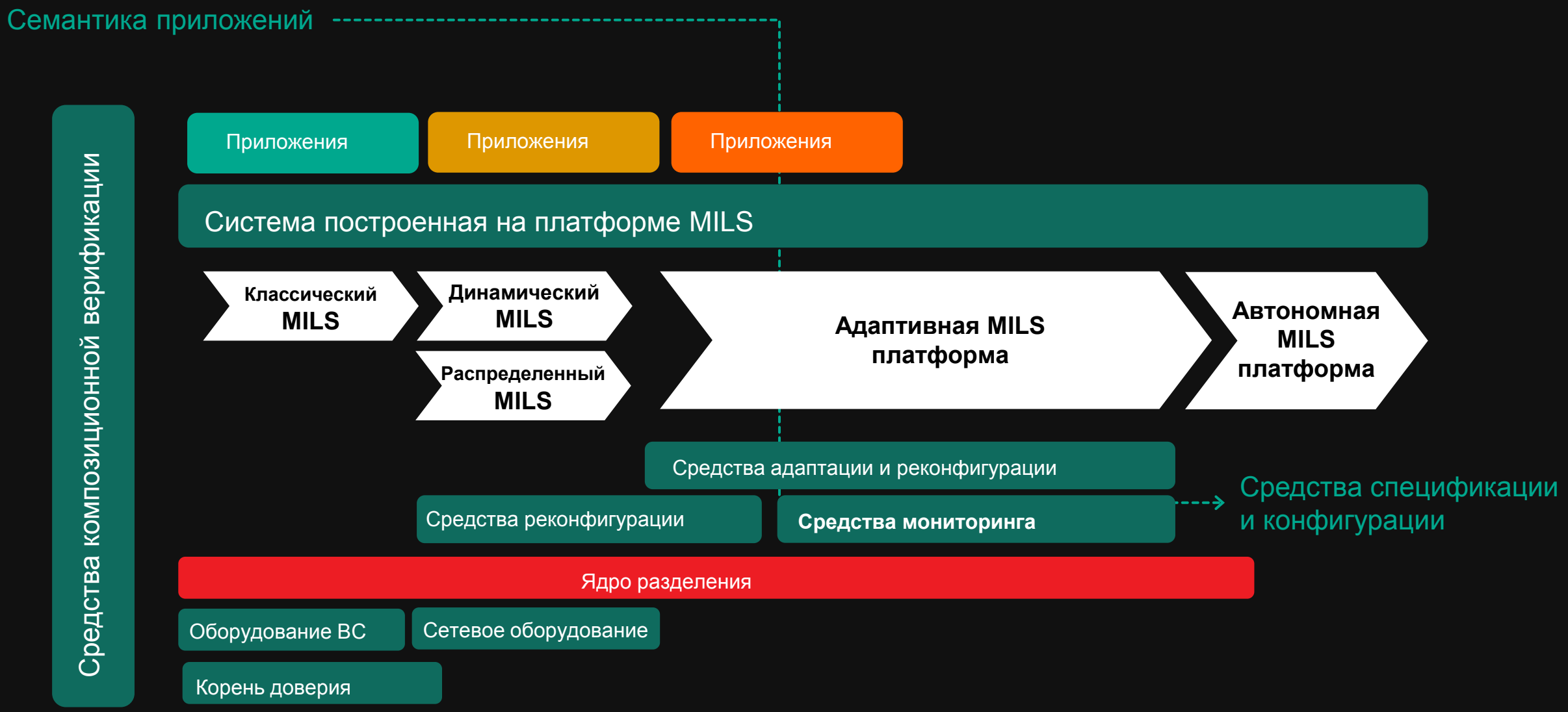
Большинство систем КИИ сложны и оттого хрупкие, в основном не способные переносить внешние воздействия

Устойчивая система способна адаптироваться к изменениям.
Устойчивость - открытое требование, поскольку условия могут быть сколь угодно широкими



Некоторые исследования предлагают подражать биологическим системам для достижения устойчивости, подход адаптивного MILS скорее про подражание людям

Адаптивная MILS платформа



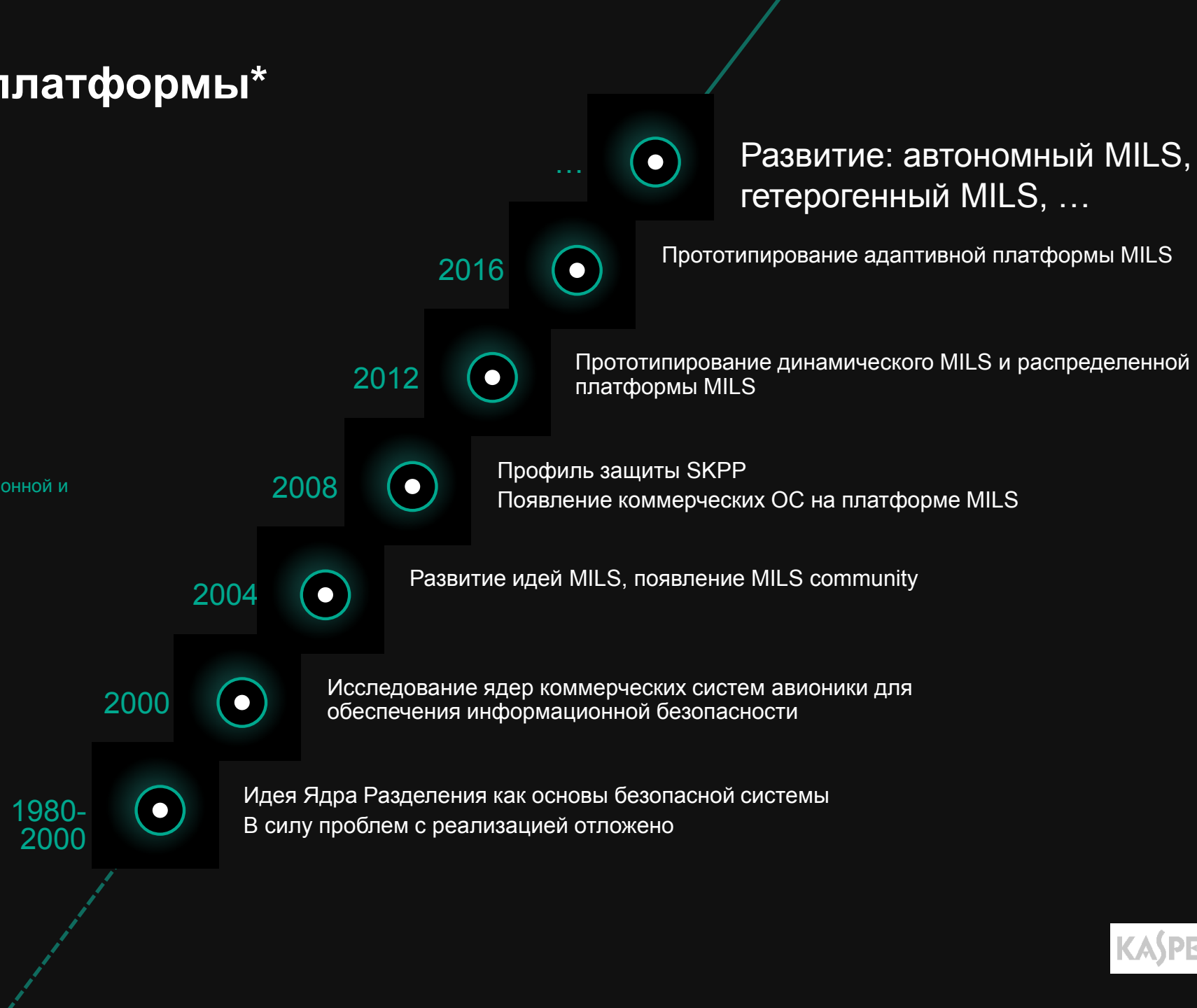
Эволюция MILS платформы*

Основная идея:

— Безопасные системы должны рассматриваться как системы распределенных компонентов
— Ядро разделения является TCB

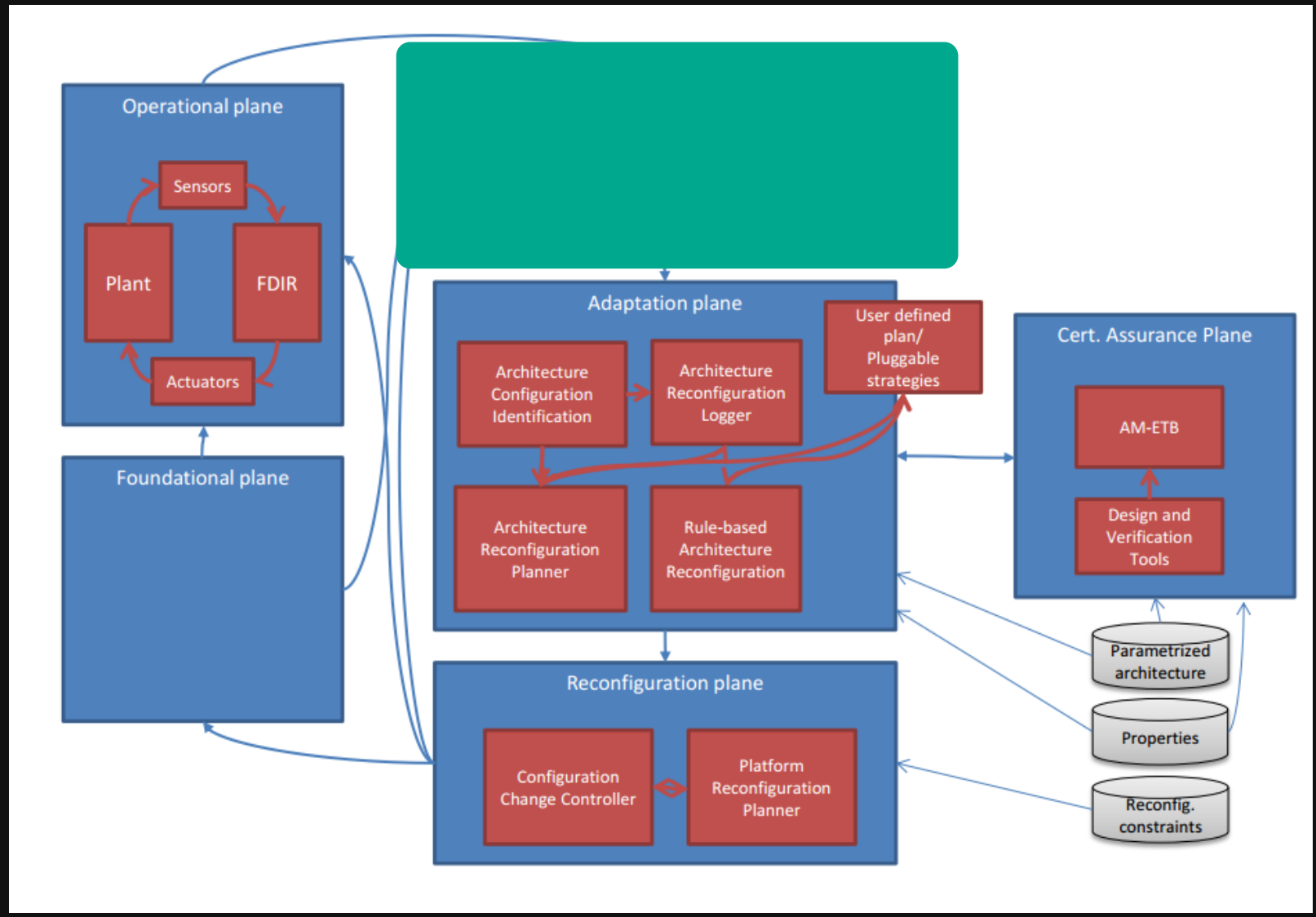
Цели:

— Одновременное обеспечение информационной и функциональной безопасности
— Упрощение валидации и верификации
— Поддержка разных политик безопасности

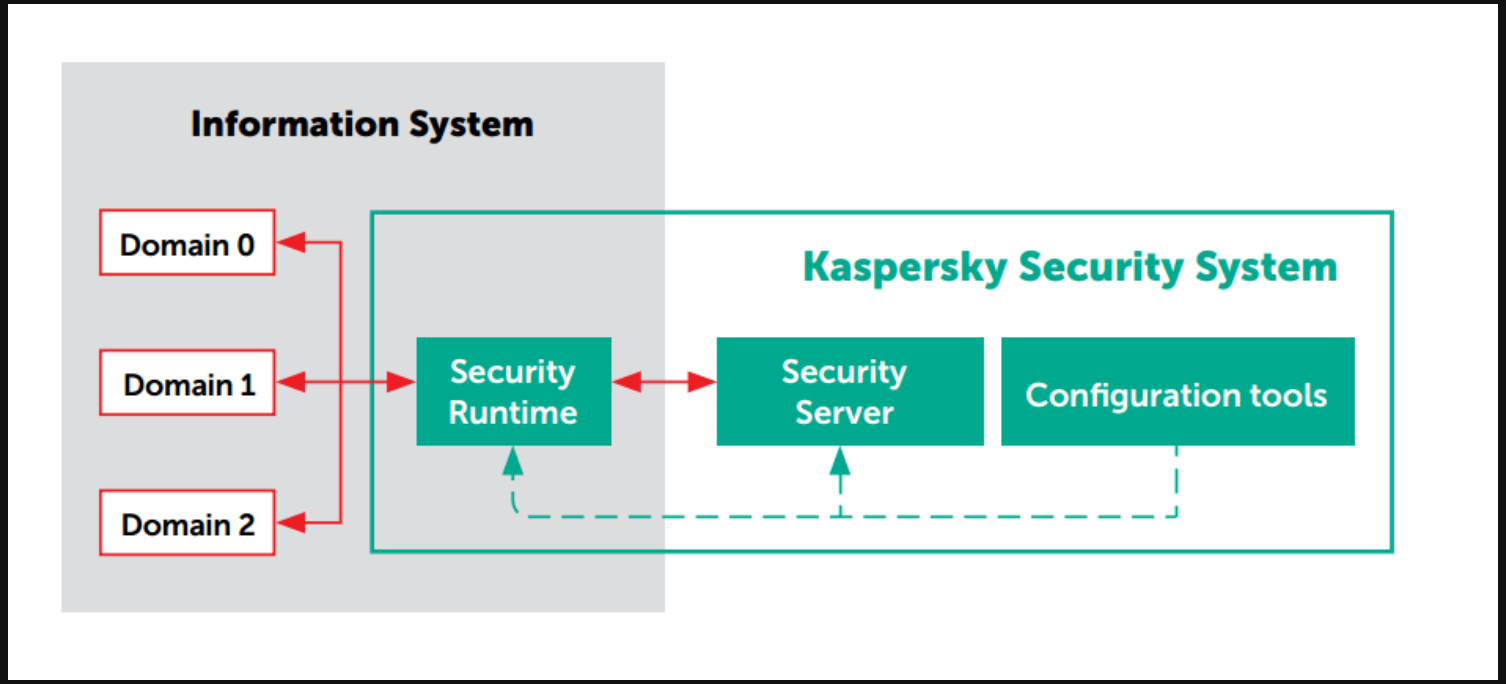


* Даты указаны приблизительно

Роль и задачи мониторинга состояний

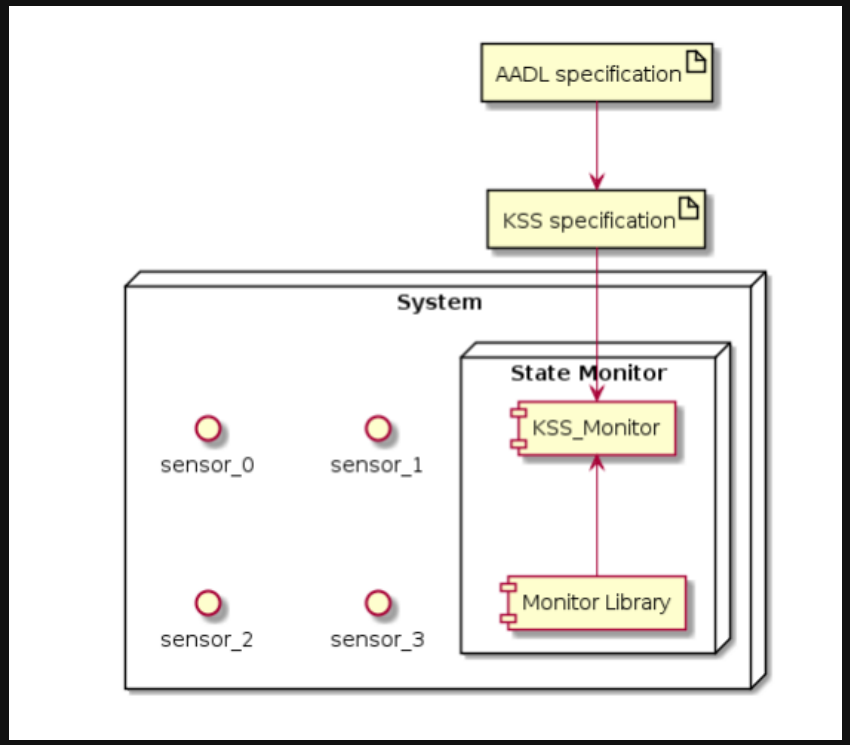


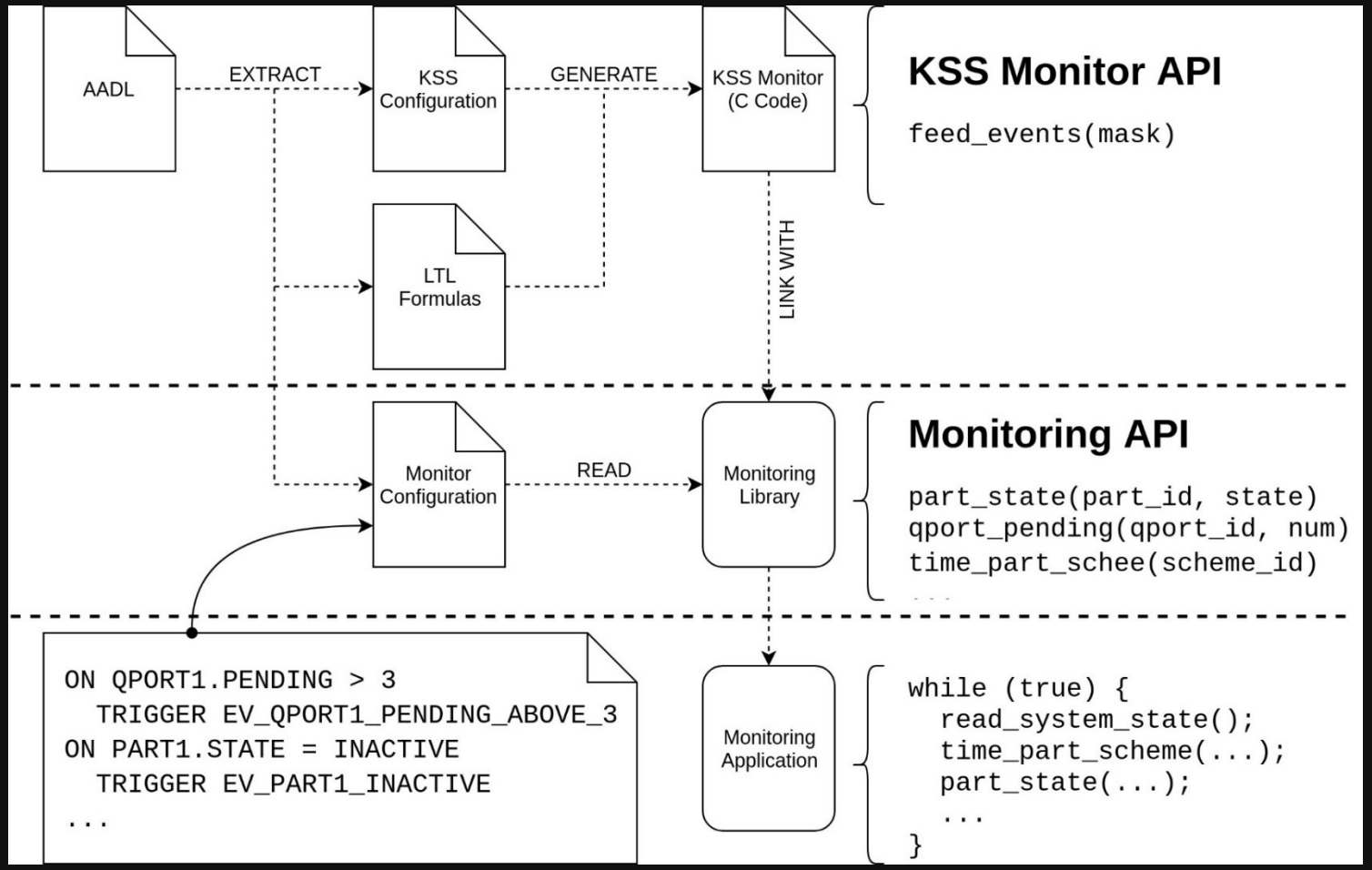
Механизм мониторинга состояний на основе Kaspersky Security System



KSS позволяет реализовать уникальные политики безопасности (в данном случае мониторинга) в каждом конкретном случае ее применения
Поддержка неиспользуемых политик в систему не включается, подсистема безопасности в каждом случае применения обеспечивает только необходимый функционал
Возможности конфигурации и реконфигурации отвечают требованиям адаптивной MILS платформы

Интеграция KSS в адаптивную MILS платформу в качестве механизма мониторинга состояний





Неформальные требования к техпроцессу вида:

- В процессе работы промышленной установки режим управления отключен
- Одновременно может могут быть запущены не более двух установок
- Если срабатывание затвора было вызвано более 9 раз за минуту, отключить установку
- Время перед запуском системы после перебоя питания и открытием затвора должно составлять не менее 5 минут

Формальные политики

Проверка граничных условий

Сигнатуры

Линейная темпоральная логика

...

Авторизация доступа

Метрическая темпоральная логика

Счетчики

Подводные камни проекта

Разная технологическая зрелость

Границы ответственности

Полнота реализации

Интеграция

Усложненное взаимодействие

Внешний контроль

Много бумажной работы

Заключение