



# Мониторинг состояний системы, построенной на основе адаптивной MILS платформы

Екатерина Рудина  
Лаборатория Касперского

# Содержание

1. Обзор архитектуры MILS
2. Адаптивная MILS платформа
3. Роль и задачи мониторинга состояний
4. Механизм мониторинга состояний на основе Kaspersky Security System
5. Политики мониторинга состояний
6. Проблемы реализации
7. Заключение

# 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

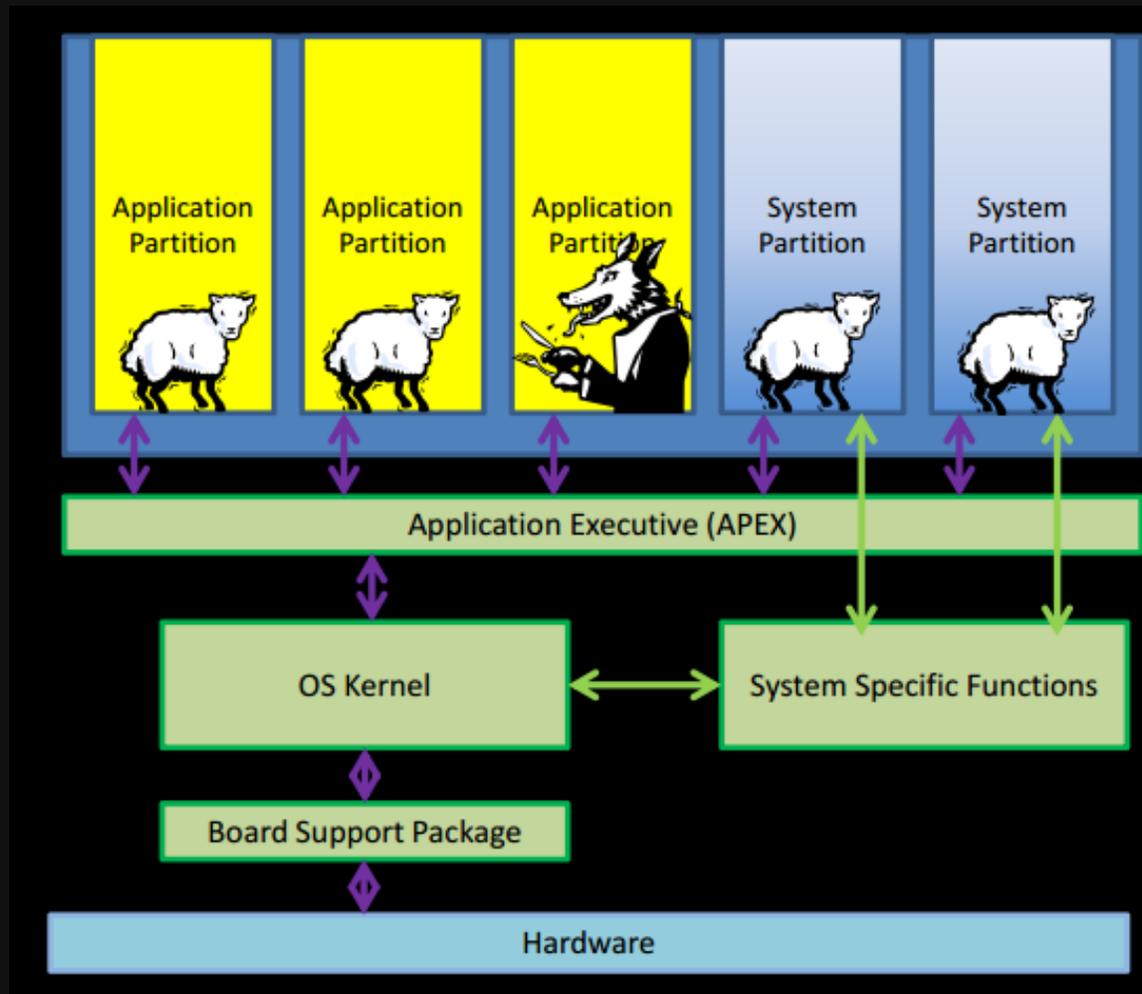
Цели:

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



\* Даты указаны приблизительно

# Другой источник



NASA Independent  
Verification and  
Validation Facility

## V&V of Integrated Modular Avionics and Partitioned Flight Software

August 13, 2012

Kimberly A. Mittelsted  
NASA IV&V Program

ИСТОЧНИК:

[https://www.nasa.gov/sites/default/files/3-5b-2012\\_workshop\\_presentation\\_on\\_arinc\\_653\\_20120822\\_submitted\\_pdf.pdf](https://www.nasa.gov/sites/default/files/3-5b-2012_workshop_presentation_on_arinc_653_20120822_submitted_pdf.pdf)

# Ожидания - реальность



## Idealized Architecture Comparison

NASA Independent  
Verification and  
Validation Facility

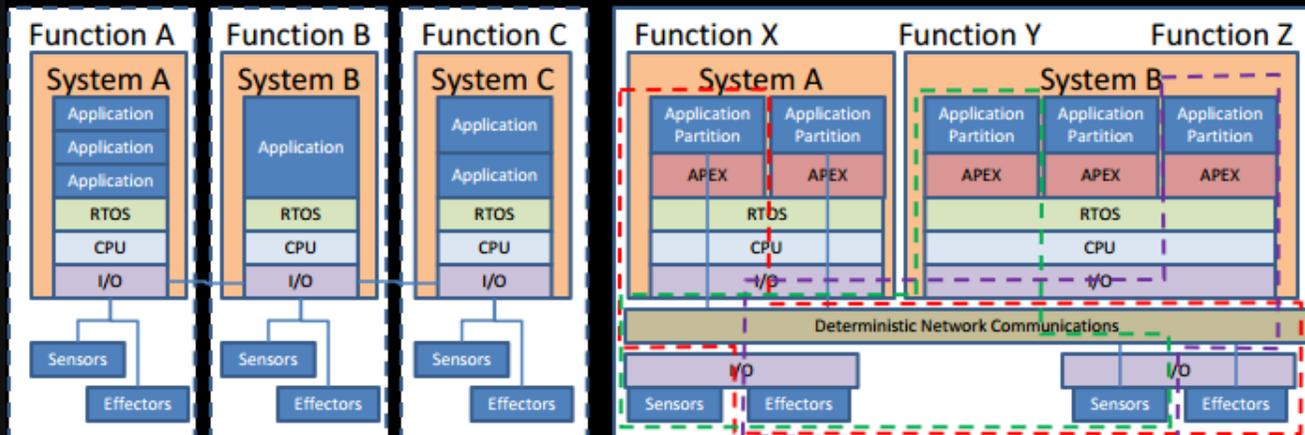
IV&V

### Federated

- Dedicated processors.
- Dedicated resources
- Lower CM complexity
- Platform dependent applications.
- Redundancy managed at box level.

### IMA

- Smaller # of processors
- Shared resources
- Platform independent application
- Portable applications
- Expandable/Reconfigurable
- Redundancy managed at IMA.



ИСТОЧНИК:

[https://www.nasa.gov/sites/default/files/3-5b-2012\\_workshop\\_presentation\\_on\\_arinc\\_653\\_20120822\\_submitted\\_pdf.pdf](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



\* Даты указаны приблизительно

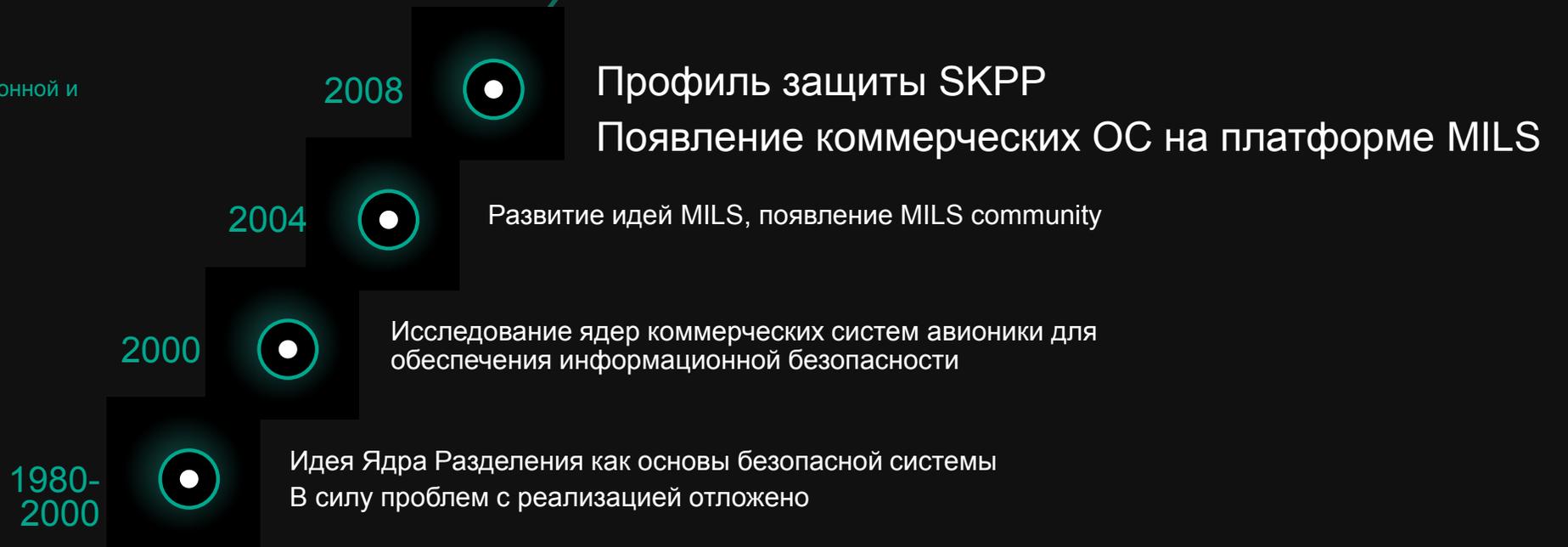
# Эволюция MILS платформы\*

Основная идея:

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

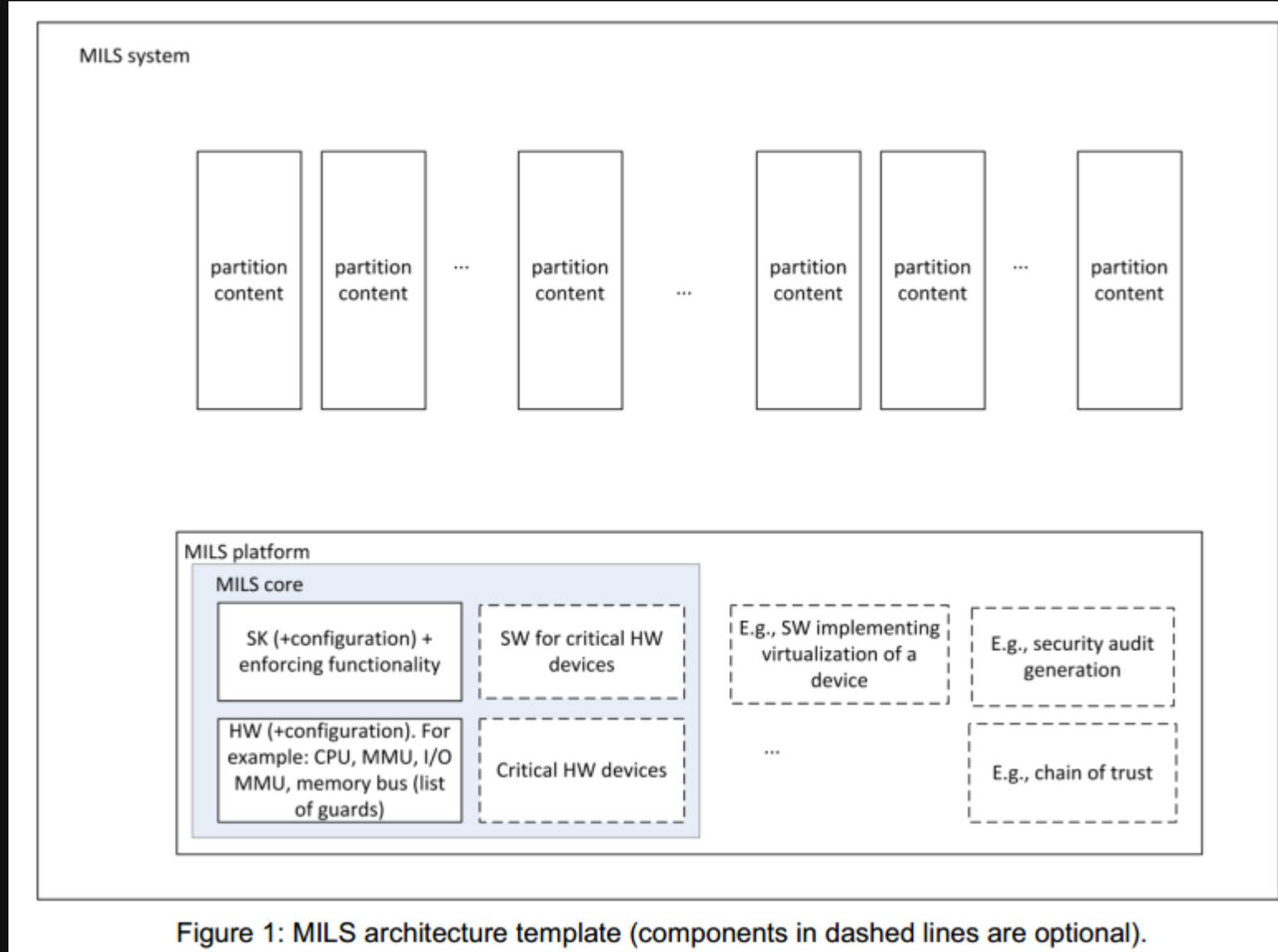
Цели:

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



\* Даты указаны приблизительно

# Система, построенная на основе платформы MILS



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



\* Даты указаны приблизительно

# MILS платформа: архитектура доверия

## MILS Policy Architecture



The architecture expresses an interaction policy among a collection of components

Circles represent architectural components (subjects / objects)

The absence of an arrow is as significant as the presence of one

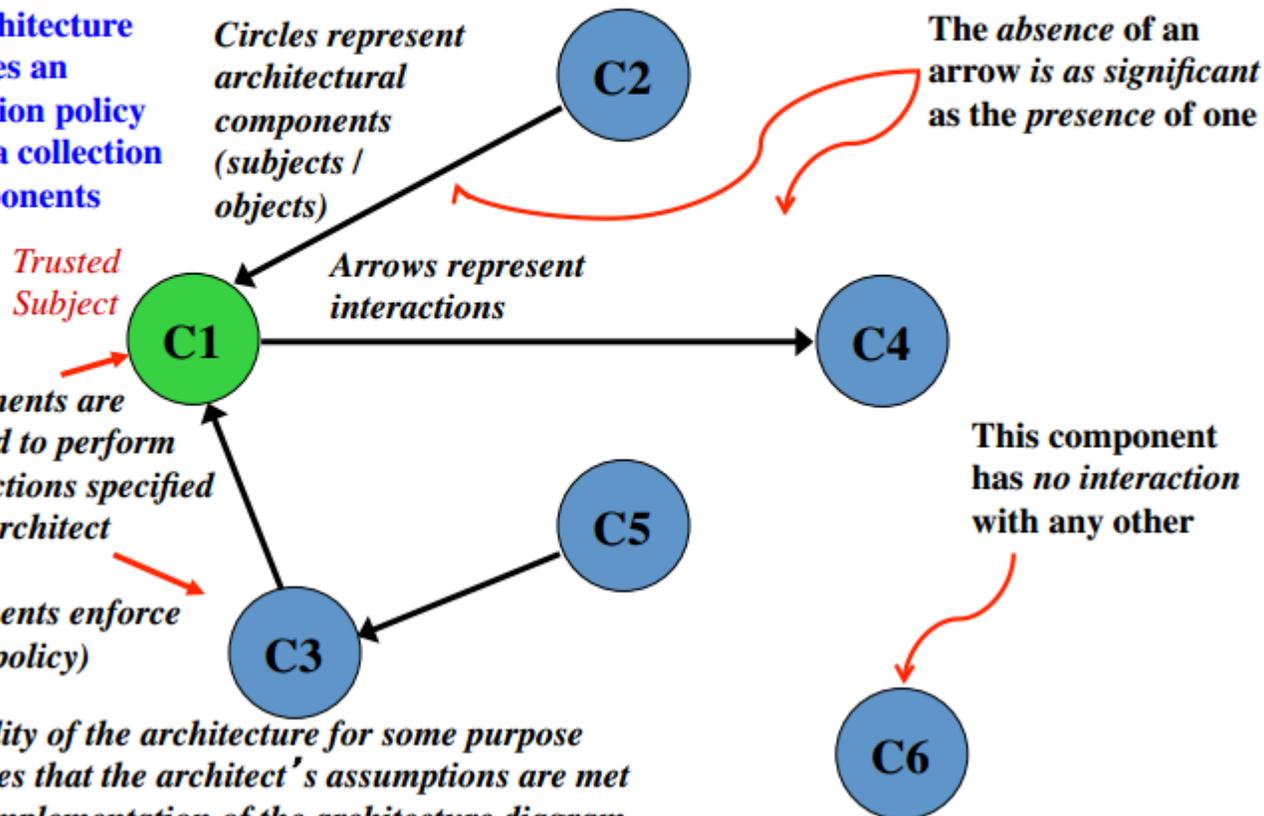
Trusted Subject

Arrows represent interactions

Components are assumed to perform the functions specified by the architect (trusted components enforce a local policy)

This component has no interaction with any other

Suitability of the architecture for some purpose presumes that the architect's assumptions are met in the implementation of the architecture diagram.

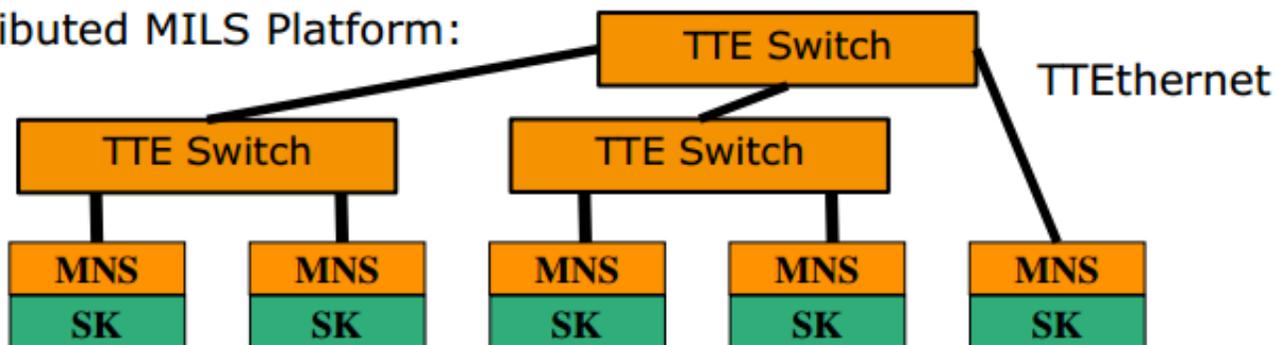


# Распределенная MILS платформа

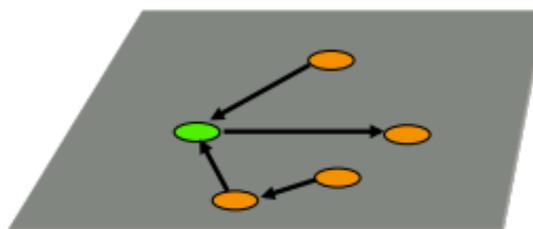
## Distributed MILS Platform – MILS nodes with deterministic communication



A Distributed MILS Platform:



Enables:



Realization of  
deterministic  
distributed MILS  
architectures



# 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

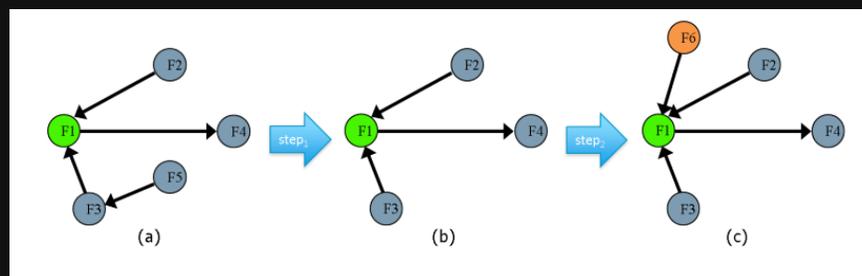
# Динамический MILS и Адаптивная MILS платформа для обеспечения устойчивости критической инфраструктуры

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

Семантика приложений



# Эволюция MILS платформы\*

## Основная идея:

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

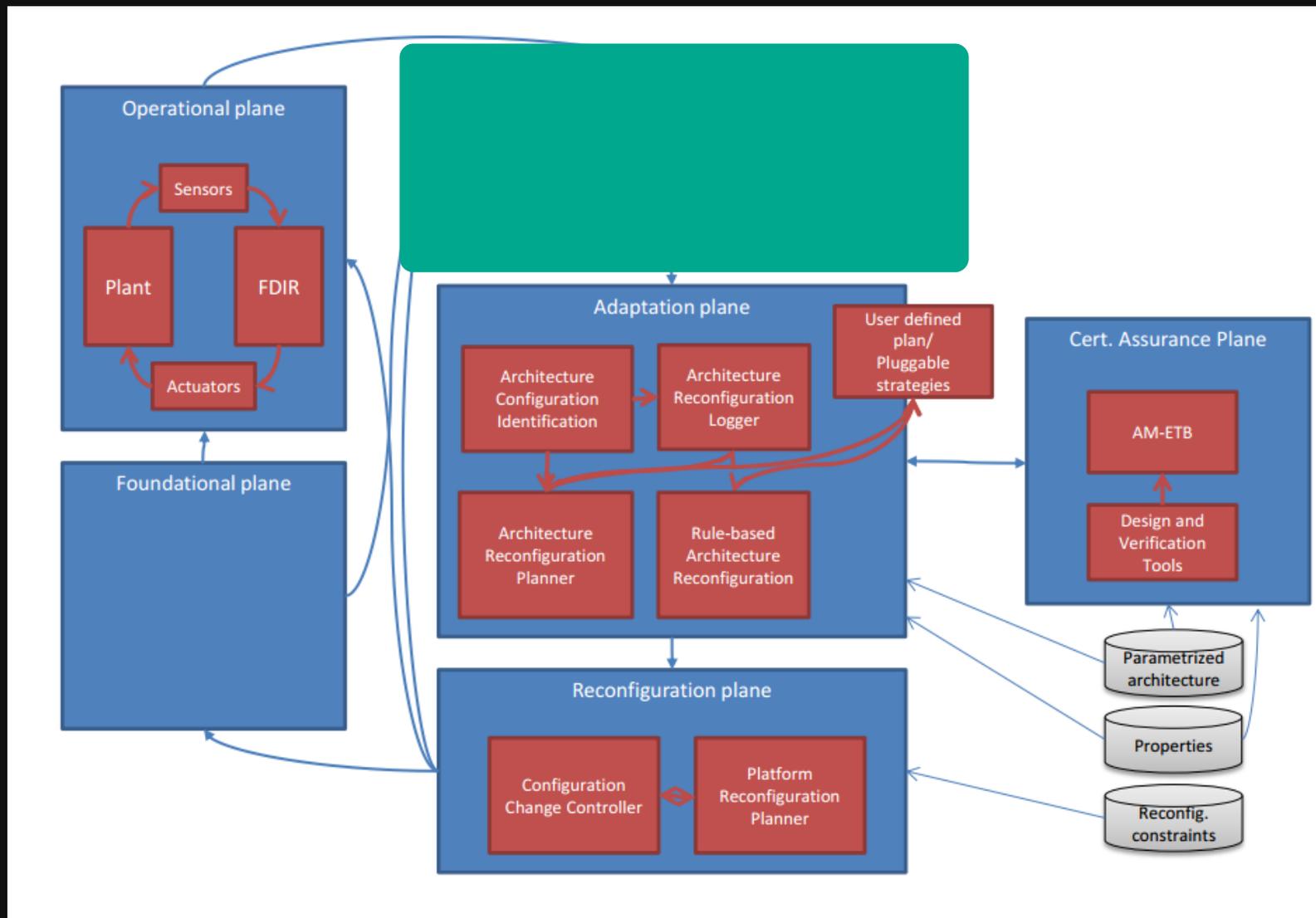
## Цели:

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

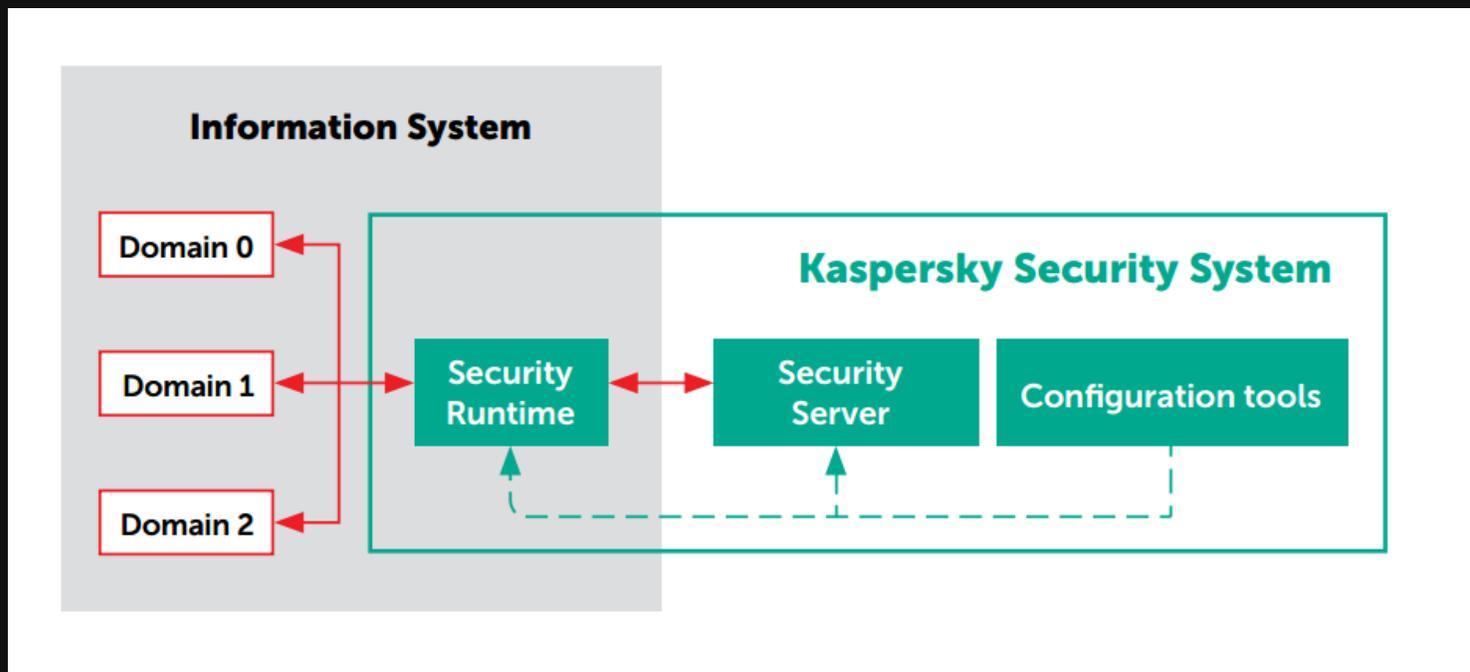


\* Даты указаны приблизительно

# Роль и задачи мониторинга состояний



# Механизм мониторинга состояний на основе Kaspersky Security System

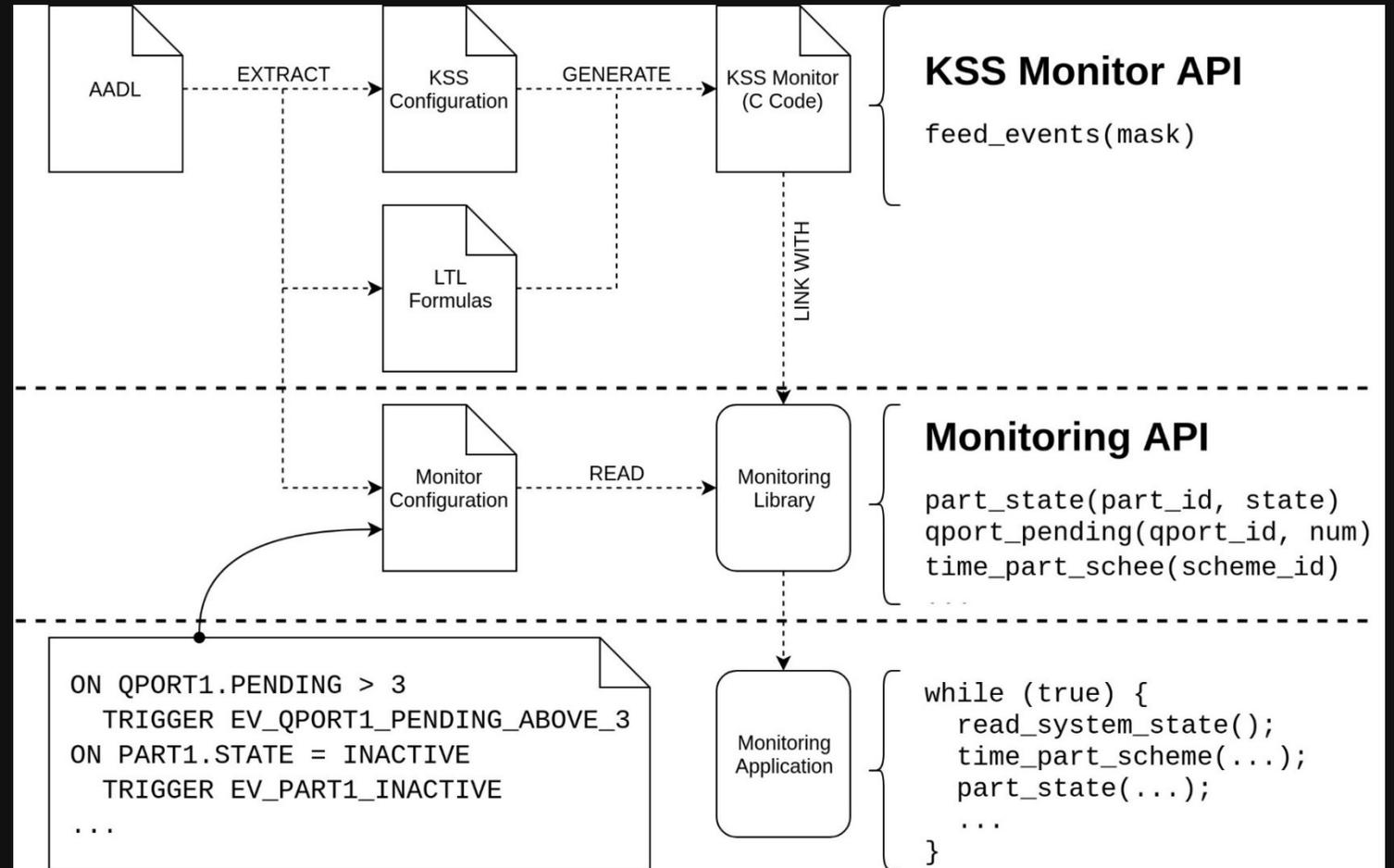
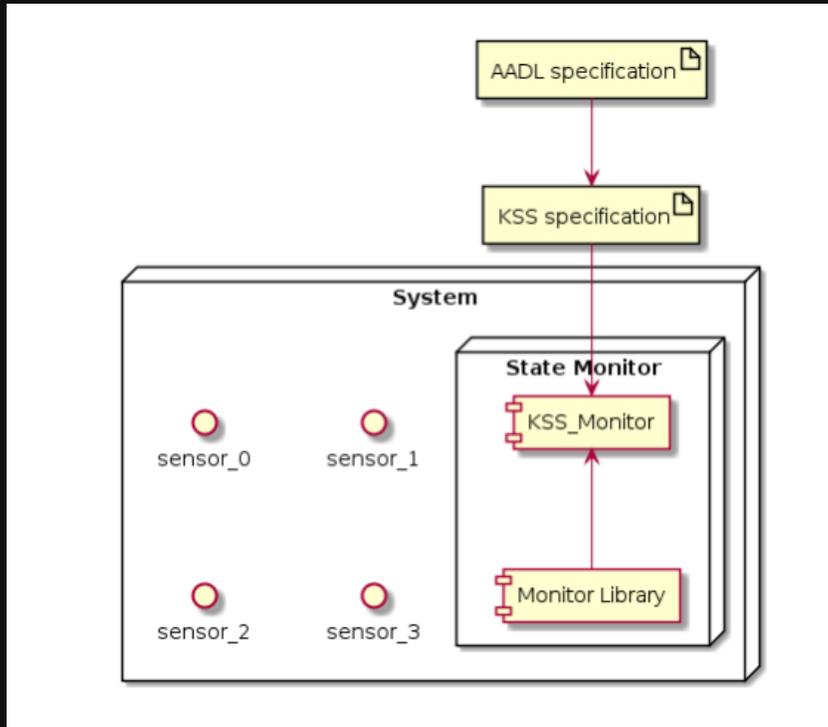


KSS позволяет реализовать уникальные политики безопасности (в данном случае мониторинга) в каждом конкретном случае ее применения

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 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