ПОСТРОЕНИЕ ПЛАТФОРМЫ БЕЗОПАСНОСТИ ПЕРСПЕКТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ НА АРХИТЕКТУРЕ RISC-V ДЛЯ СОВРЕМЕННЫХ ОС

Никита Диваков, Павел Габер

June, 2024

Угрозы безопасности

	Privilege Levels	Stack	Pointer Authentication	Branch Predictor	Speculative, OoO Execution	CPU Cache	Shared Cache	Line Fill Buffer	Data Prefetcher	Ext. TPM	DMA
Buffer Overflow		X									
Downfall	X				X						
CacheWarp	X						X				
PACMAN			X		X	X					
Pathfinder				X							
Retbleed				X		X	X				
Spectre				X	X	X	X				
Meltdown					X	X	X				
Foreshadow					X	X					
GoFetch, Augury						X			X		
RIDL					X		X	X			
ZombieLoad					X	X	X	X			
faulTPM										X	
TPM2.0 Out-of-bounds										X	
0wned by an iPod											X
Ghost in the Wireless											X
PCILeech											X

Buffer overflow – 80% ошибок ПО

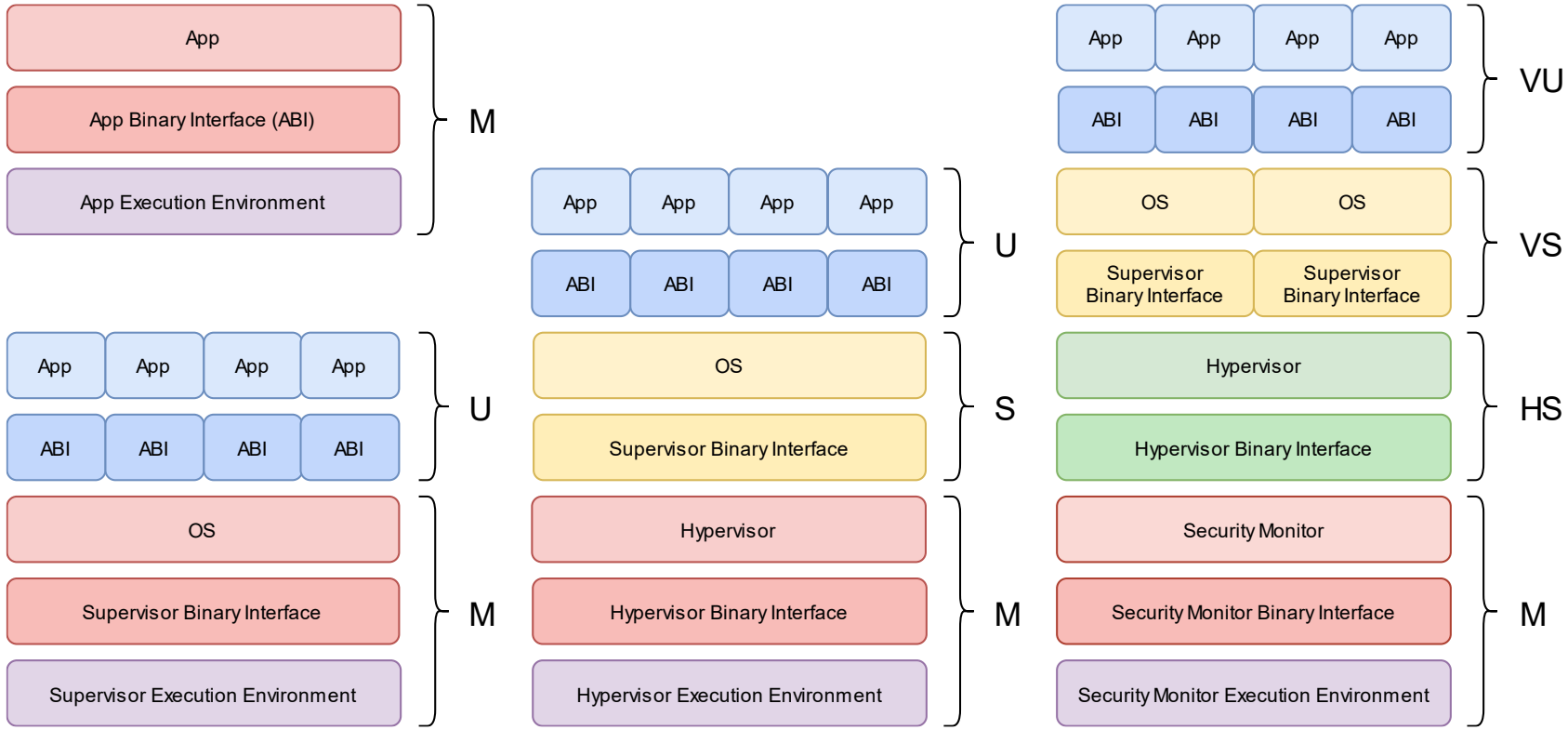
Branch predictor, speculative execution – драйверы производительности

Слабая модель защиты памяти открывает возможности атак

Практикуется игнорирование механизмов защиты в угоду производительности

Больше всего атак проводится на модули CPU

Privilege Levels, Hypervisor



M-mode - для простых микроконтроллеров

U и M-mode - для встраиваемых систем, многозадачных ОС

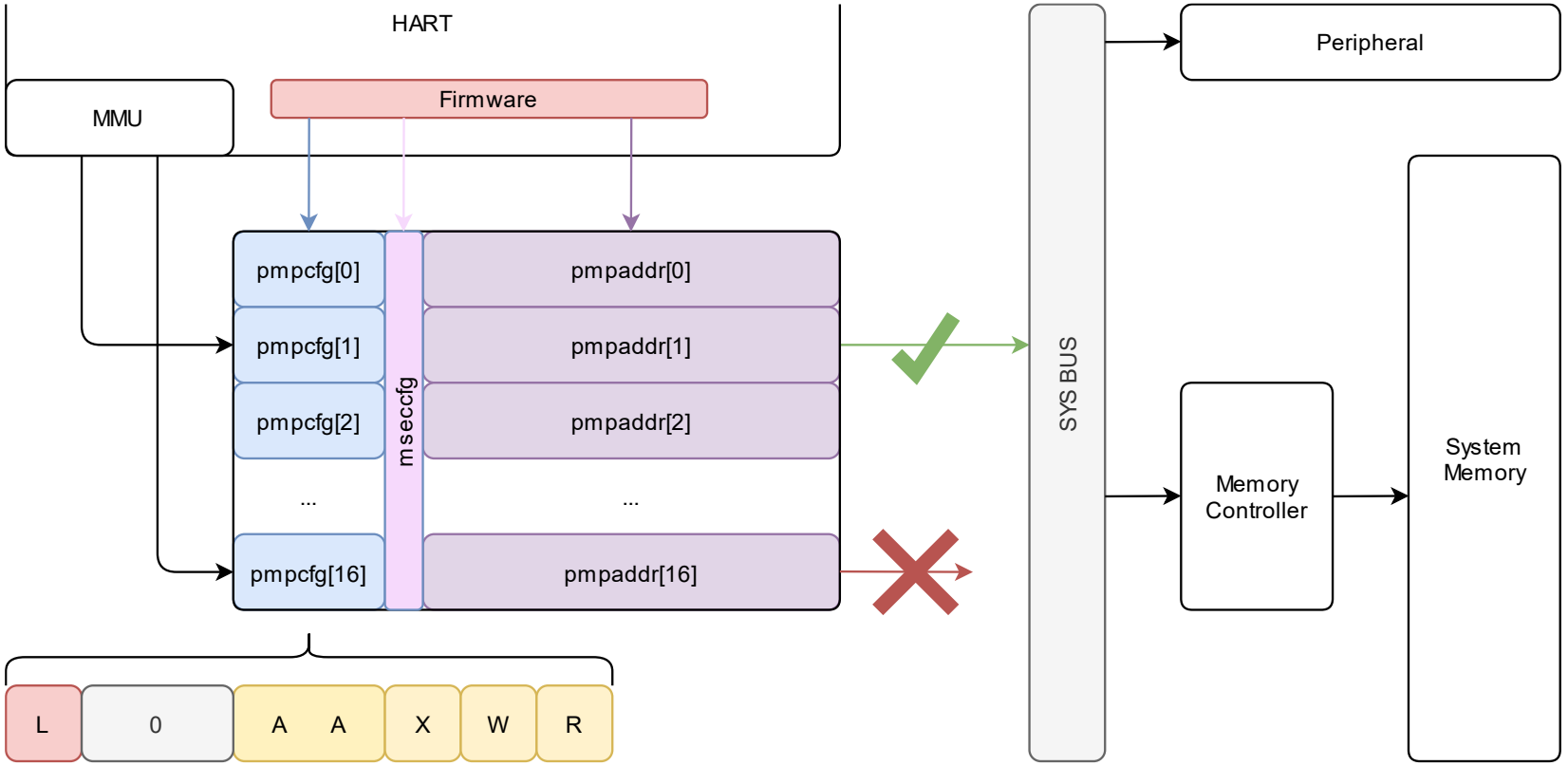
U, S и M-mode – для запуска Unix-like ОС

Расширение гипервизора:
VS-mode – виртуальный S-mode
VU-mode – виртуальный U-mode

Поддерживает многоуровневую вложенную виртуализации

Легко эмулируется программно

PMP / ePMP



До 16 регионов памяти

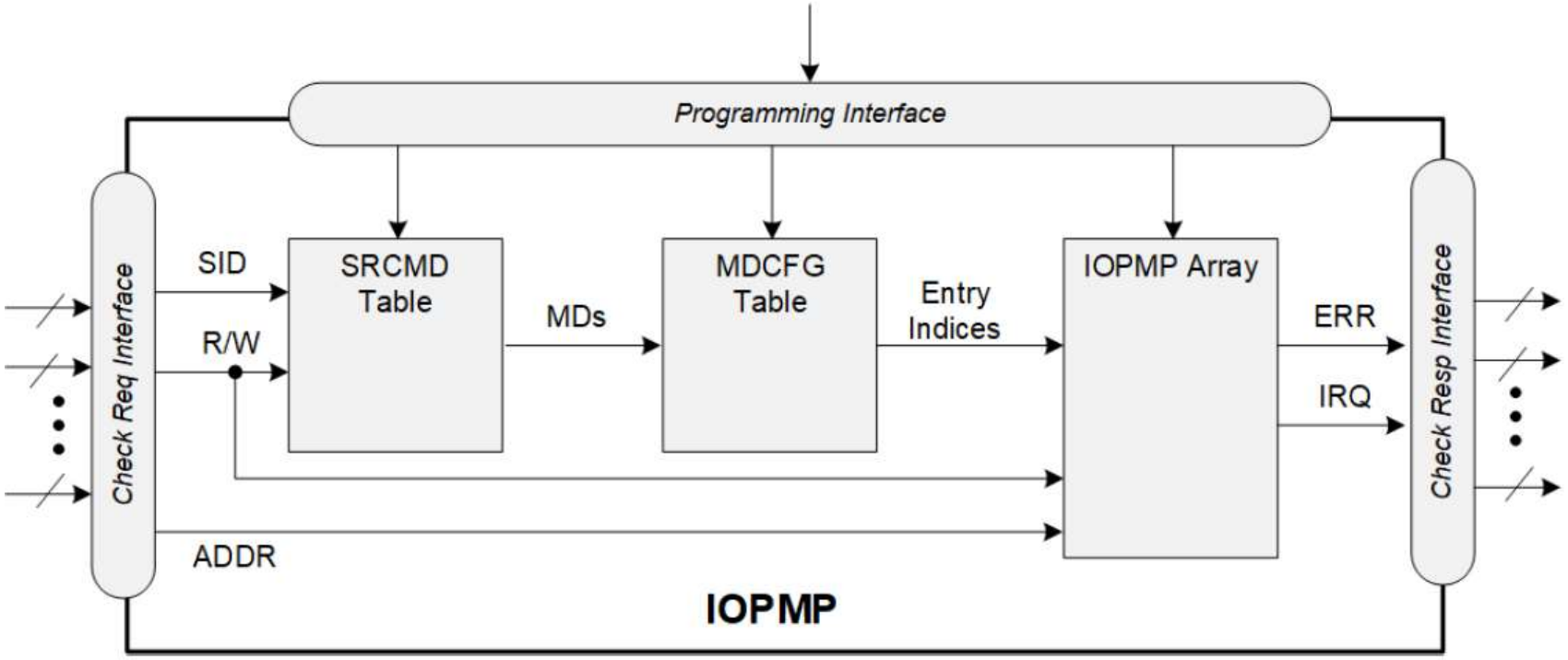
Разные права доступа для U/S и M режимов.

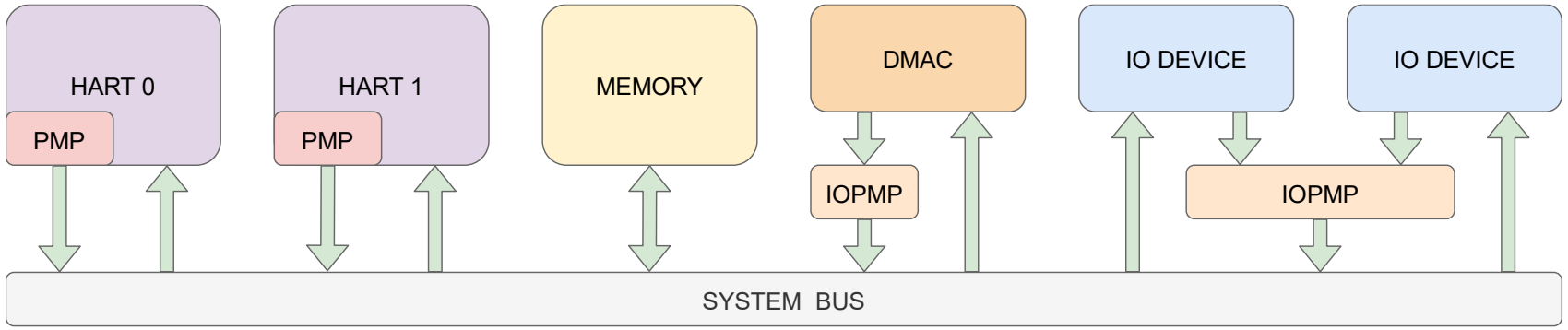
Блокировка настроек доступа до сброса PMP

PMP: Дает доступ для U/S режимов или ограничивает всем

ePMP: Добавляет ограничения для M режима

IOPMP





Проверяет запросы от периферии с DMA

Табличная структура, простая в реализации

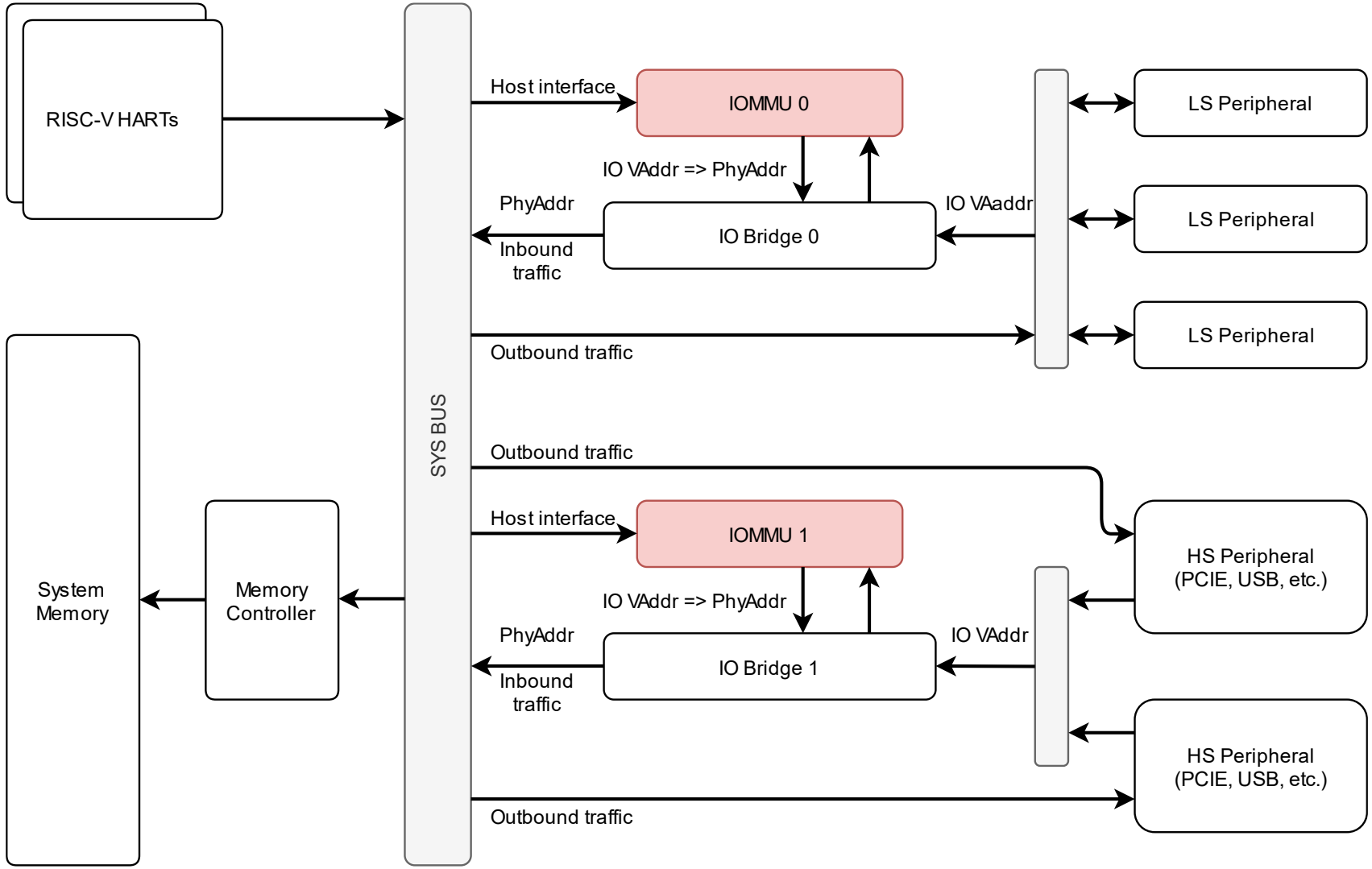
До 65535 подключенных источников запросов

До 64 доменов памяти

Гибкая настройка количества диапазонов адресов в доменах

Поддерживает упрощенные модели проверок:
Rapid-k, Compact-k, Dynamic-k

IOMMU



Дает доступ IO модулей к виртуальным адресам

Программно конфигурируемый контекст подключенных устройств

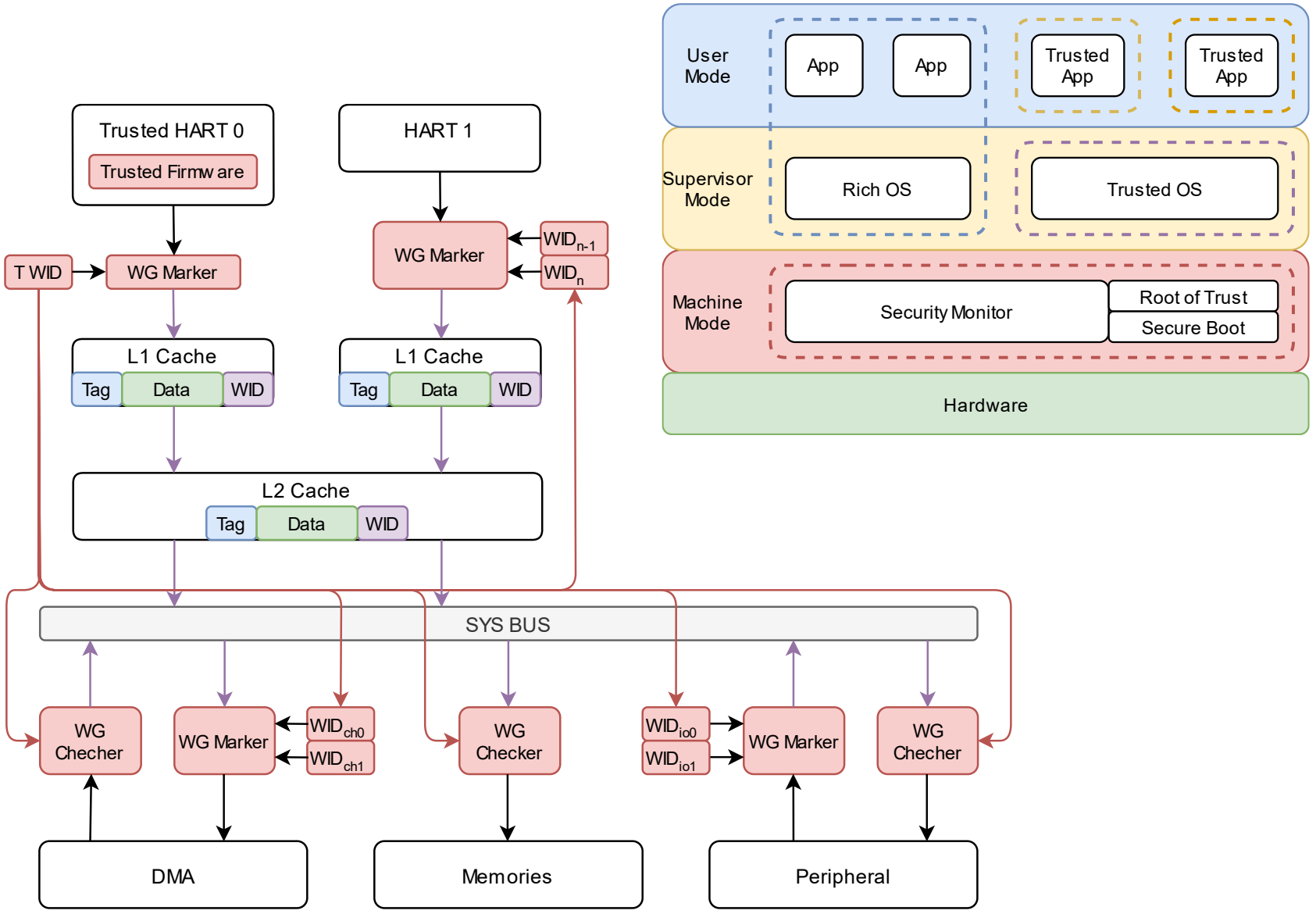
Двухэтапная трансляция адресов

Использует такие же форматы таблиц памяти, как MMU в CPU

Простое управление памятью

Обеспечивает прямой контроль гостевых ОС над IO модулями

WorldGuard



Решение от компании SiFive

Миры – изолированные приложения и их ресурсы

Изоляция на уровне физических адресов, только между «мирами»

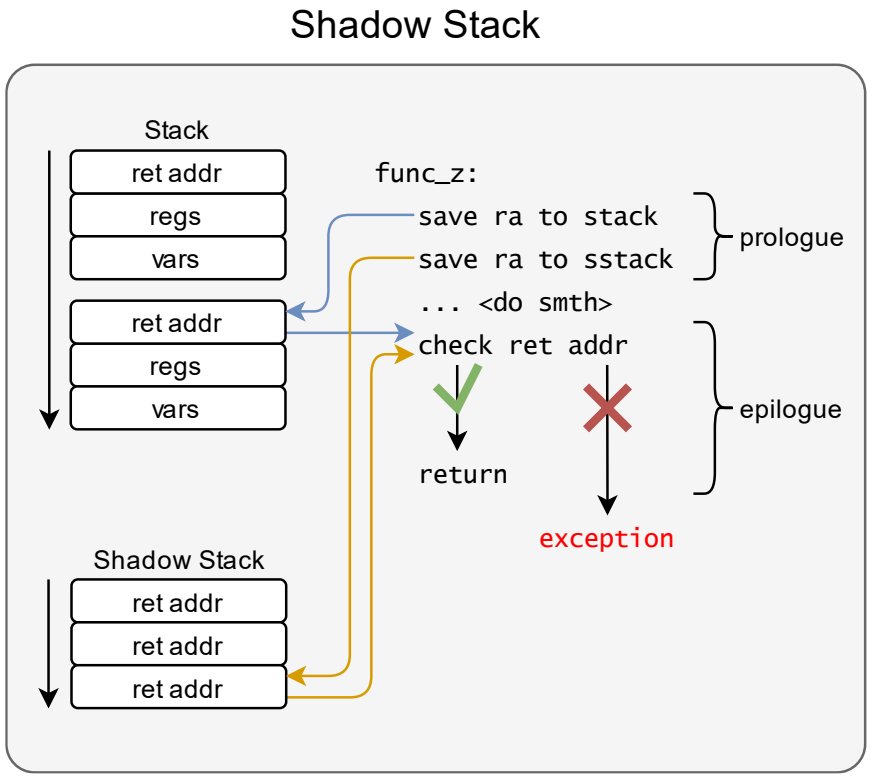
Два аппаратных блока:
WG Marker и WG Checker

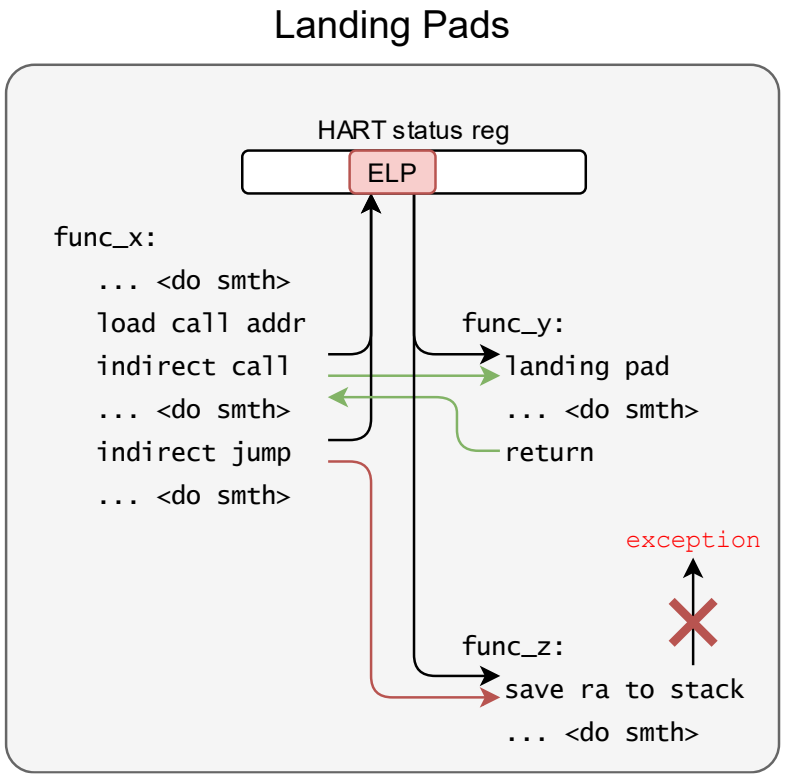
Работает совместно с PMP и MMU

Только доверенный агент может настроить блоки World Guard

Не требует изменений в RISC-V ISA

Control-flow Integrity (CFI) Capabilities





Новый регистр Shadow Stack Pointer

Новые команды SSPUSH, SSPOPCHK и SSAMOSWAP

В Shadow Stack могут писать только инструкции расширения

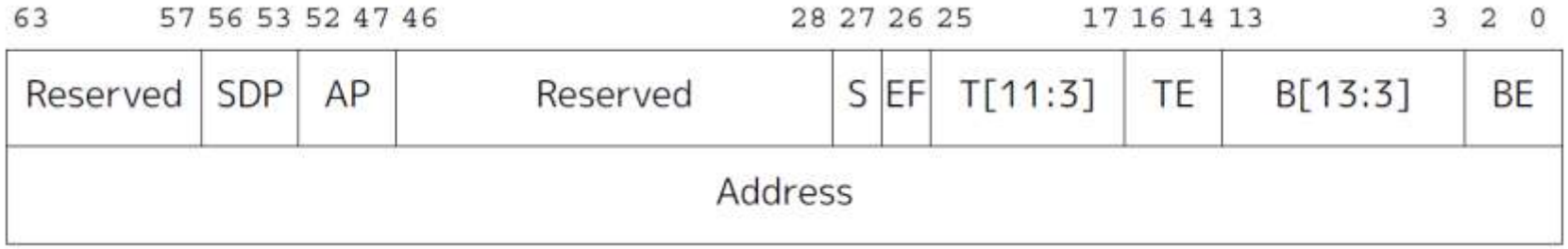
Не работает в M-mode

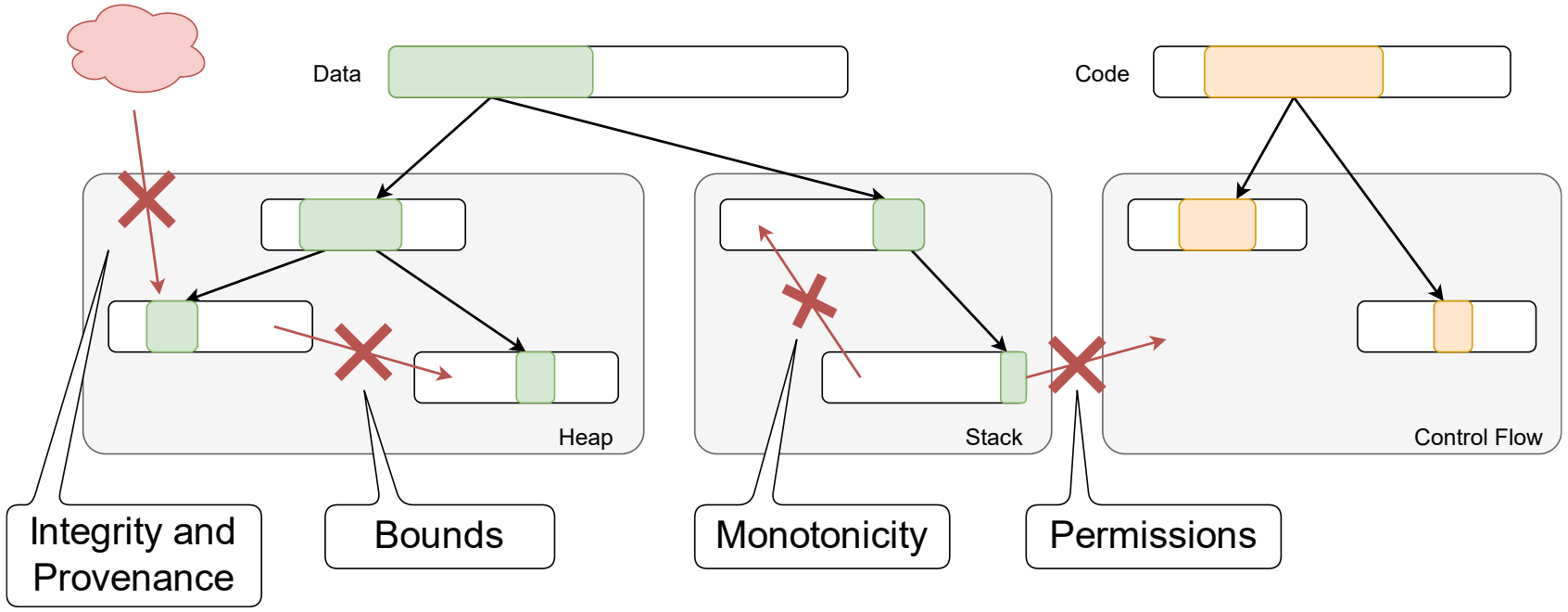
Landing Pads: новая инструкция LPAD

Контроль целей Indirect Call/Jump

Работает во всех режимах исполнения

CHERI





Набор из 5 расширений

Capability – примитив контроля доступа и модификаций адресов

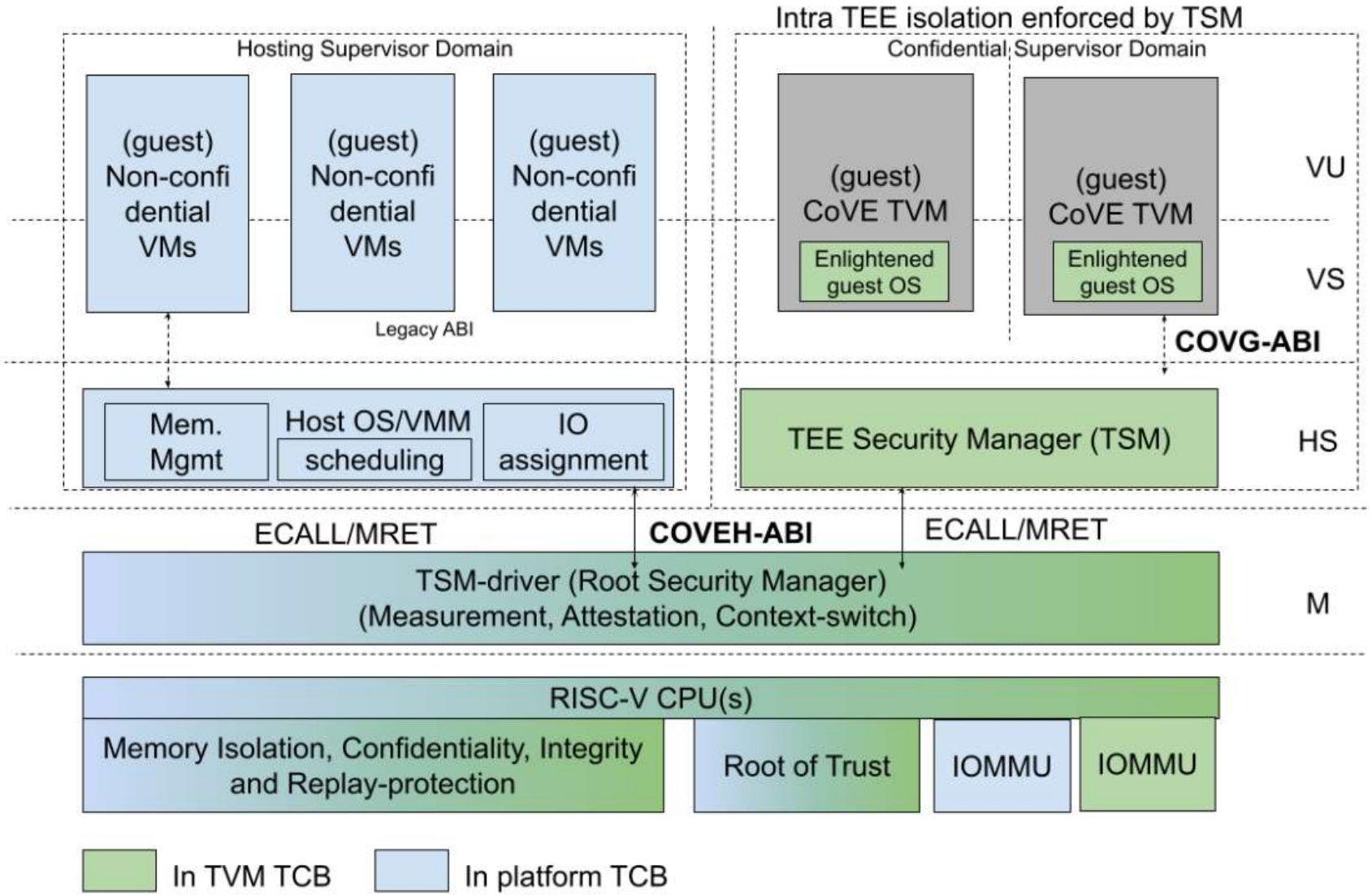
Можно задать границы изменения значений адресов

В базовом варианте не имеет обратной совместимости с RISC-V ISA

Не совместим с Shadow Stack и Landing Pads

Capabilities нельзя подделать, нельзя повысить им права

CoVE, CoVE IO



Гипервизор и доверенная виртуализация

Механизмы защиты

	Privilege Escalation	Stack	Pointer Authentication	Branch Predictor	Speculative, OoO Execution	CPU Cache	Shared Cache	Line Fill Buffer	Data Prefetcher	Ext. TPM	DMA
Hypervisor	X										
PMP / ePMP				X	X	X		X	X		
IOPMP / IOMMU										X	X
Shadow Stack		X									
Landing Pads		X	X								
CHERI		X	X	X	X	X	X	X	X	X	X
CoVE / CoVE IO	X										
WorldGuard						X	X	X	X	X	X

CHERI защищает «от всего», но сложно реализуемо и меняет ISA

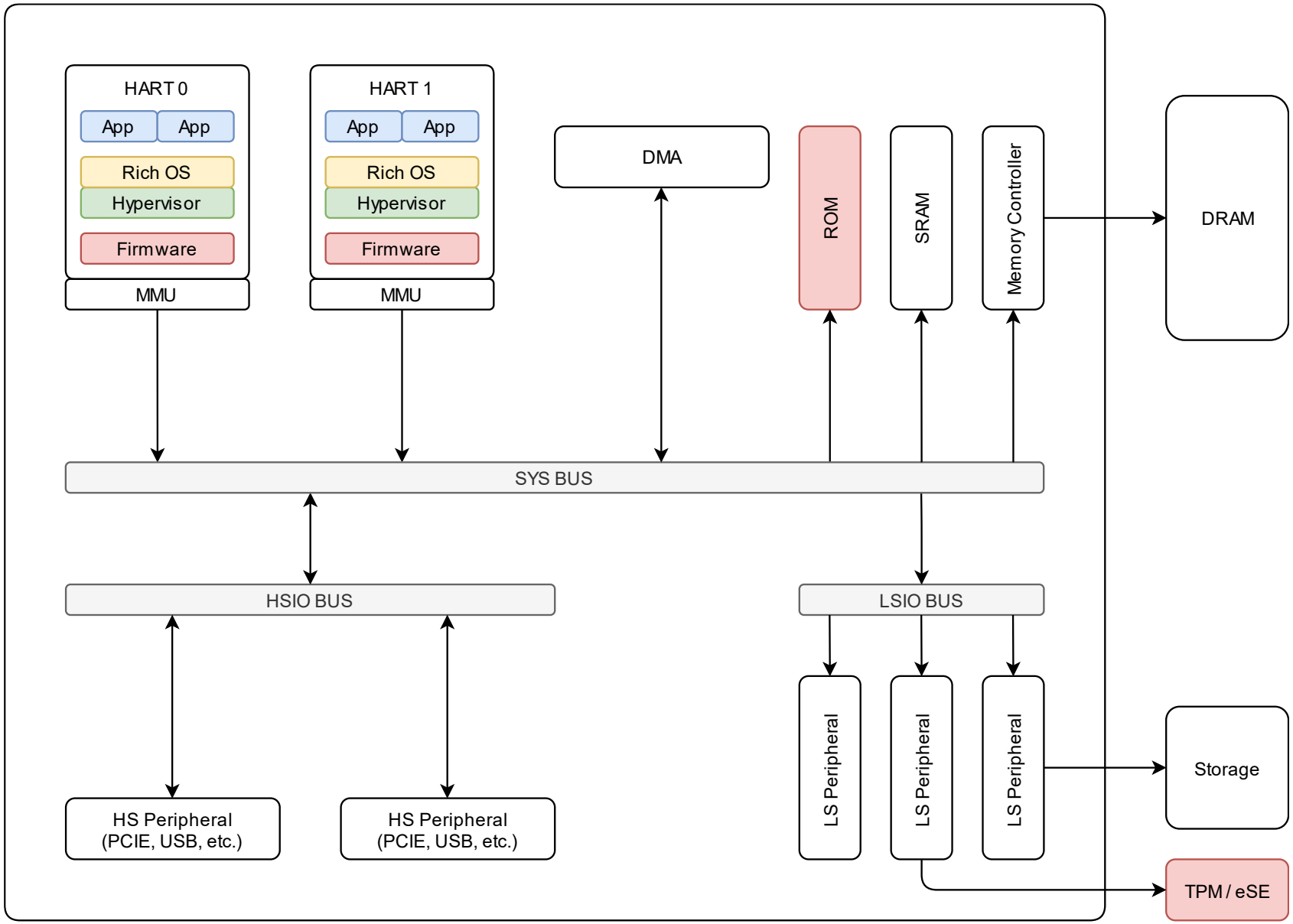
IOPMP защищает от DMA-атак

ePMP закрывает множество векторов атак на CPU (HART)

Landing Pads – эффективно и дёшево

ePMP + Shadow Stack + Landing Pads + WorldGuard как альтернатива CHERI

SoC with external TPM / eSE



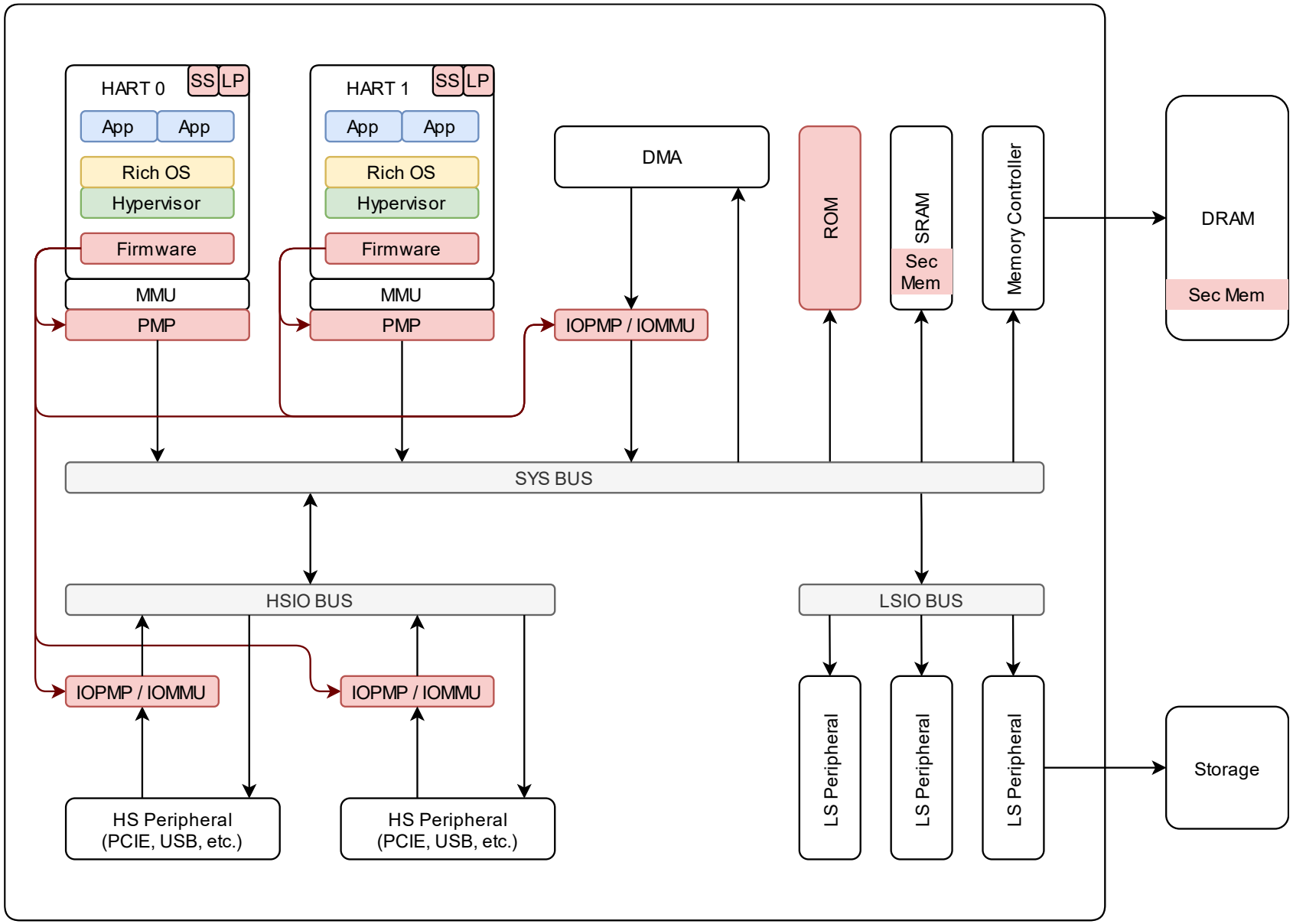
Простой способ усилить безопасность базового варианта СнК

ДСИ во внешнем периметре обеспечивает безопасное хранение и управление данными

Внешний источник доверия имеет ограниченный круг сценариев использования

Слабое место такой схемы – канал связи между СнК и модулем TPM / eSE

SoC with PMP + IOPMP



PMP + IOPMP для изоляции физических адресов

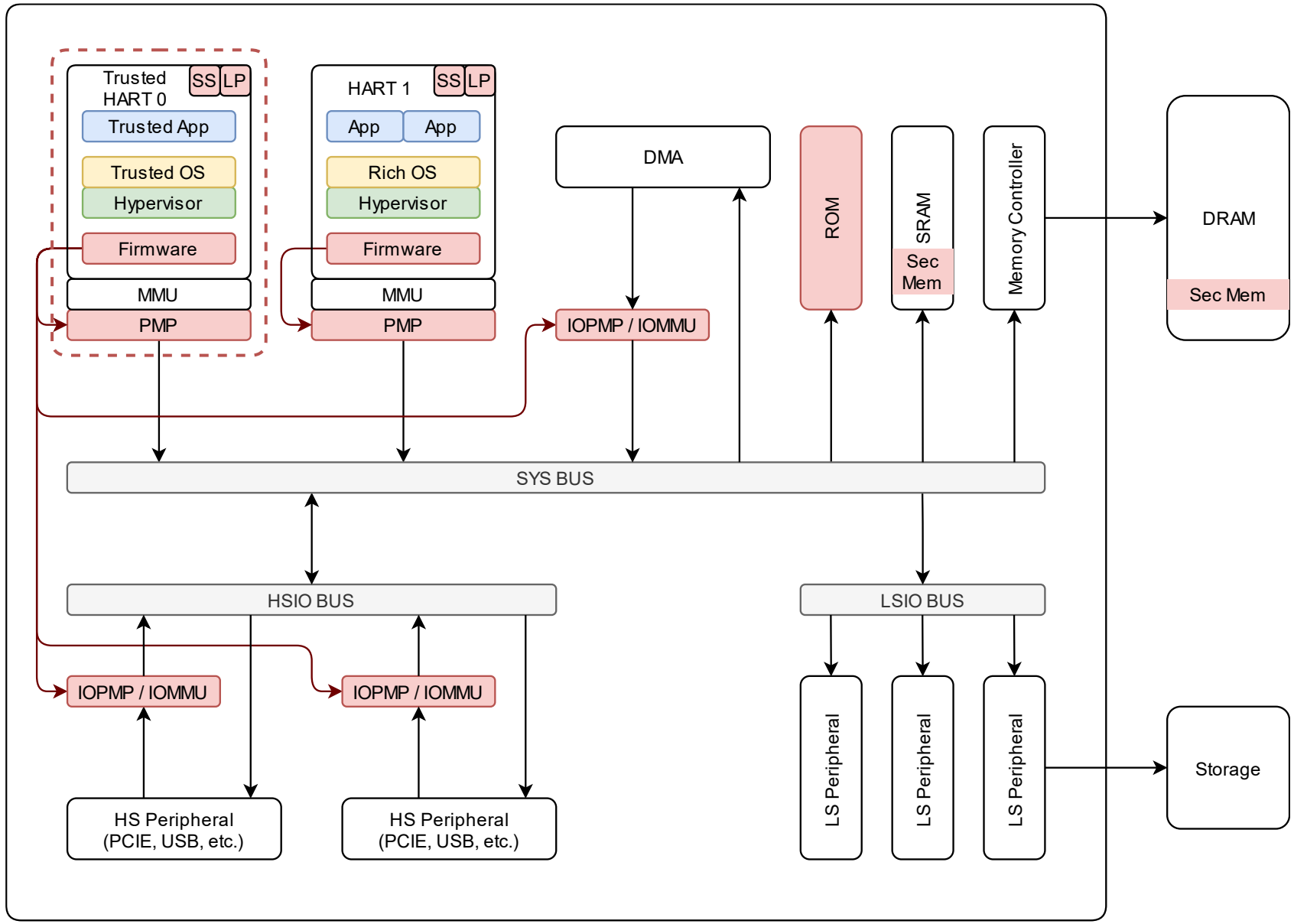
Shadow Stack и Landing Pads для контроля потока исполнения

Аппаратный корень доверия

Эскалация привилегий - высокий риск в системах с U и M-mode

Отсутствует изолированное доверенное окружение

SoC with Secured HART



Trusted HART – изолированное доверенное окружение

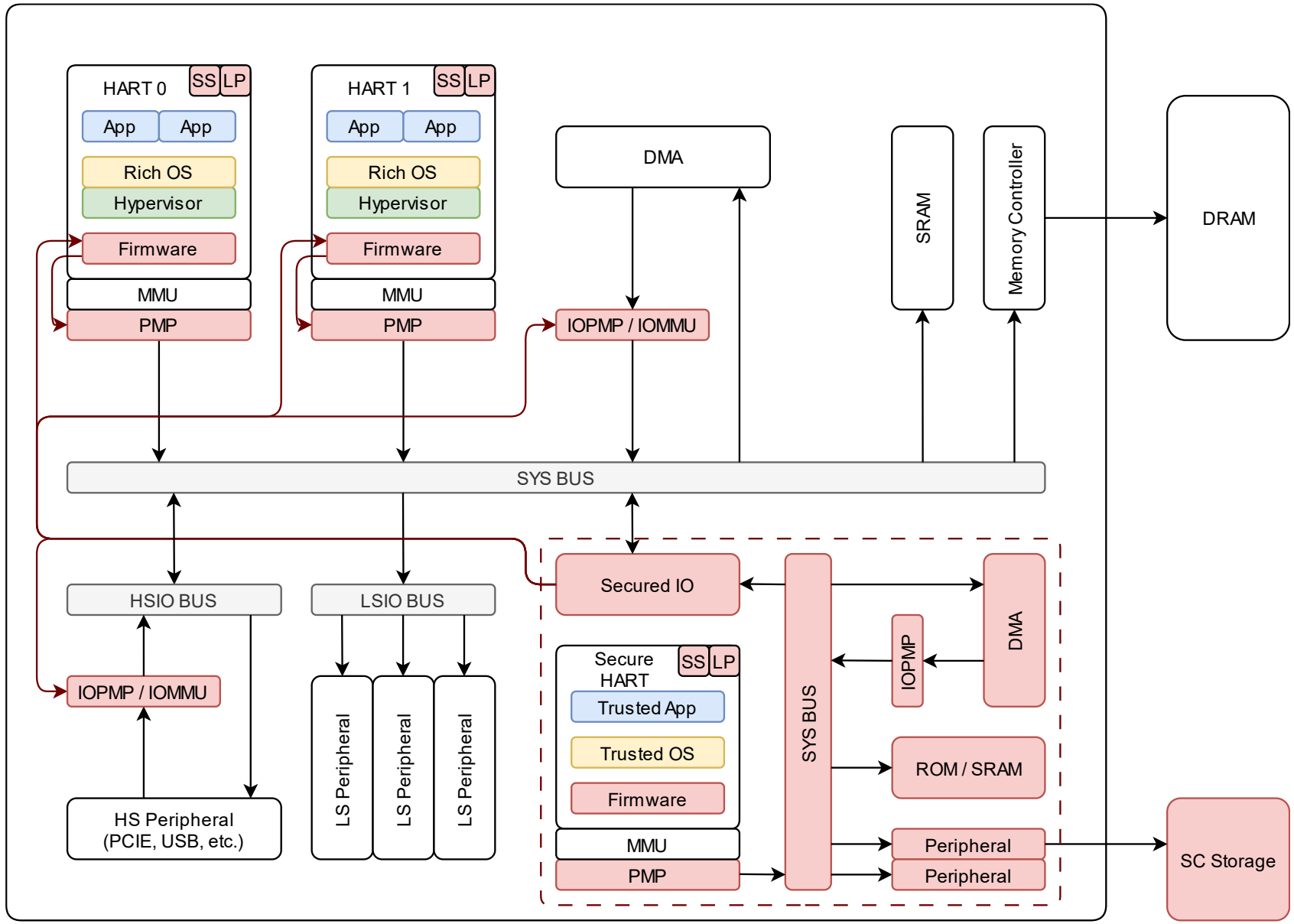
Trusted HART стартует первым

Память в пределах Trusted HART считается безопасной, остальная – условно безопасной

Только Trusted HART управляет механизмами безопасности

Производительное ядро СнК занято непрофильной задачей

SoC with Secure Subsystem



Физически изолированная подсистема ДСИ

Защищенный канал коммуникации с основной системой

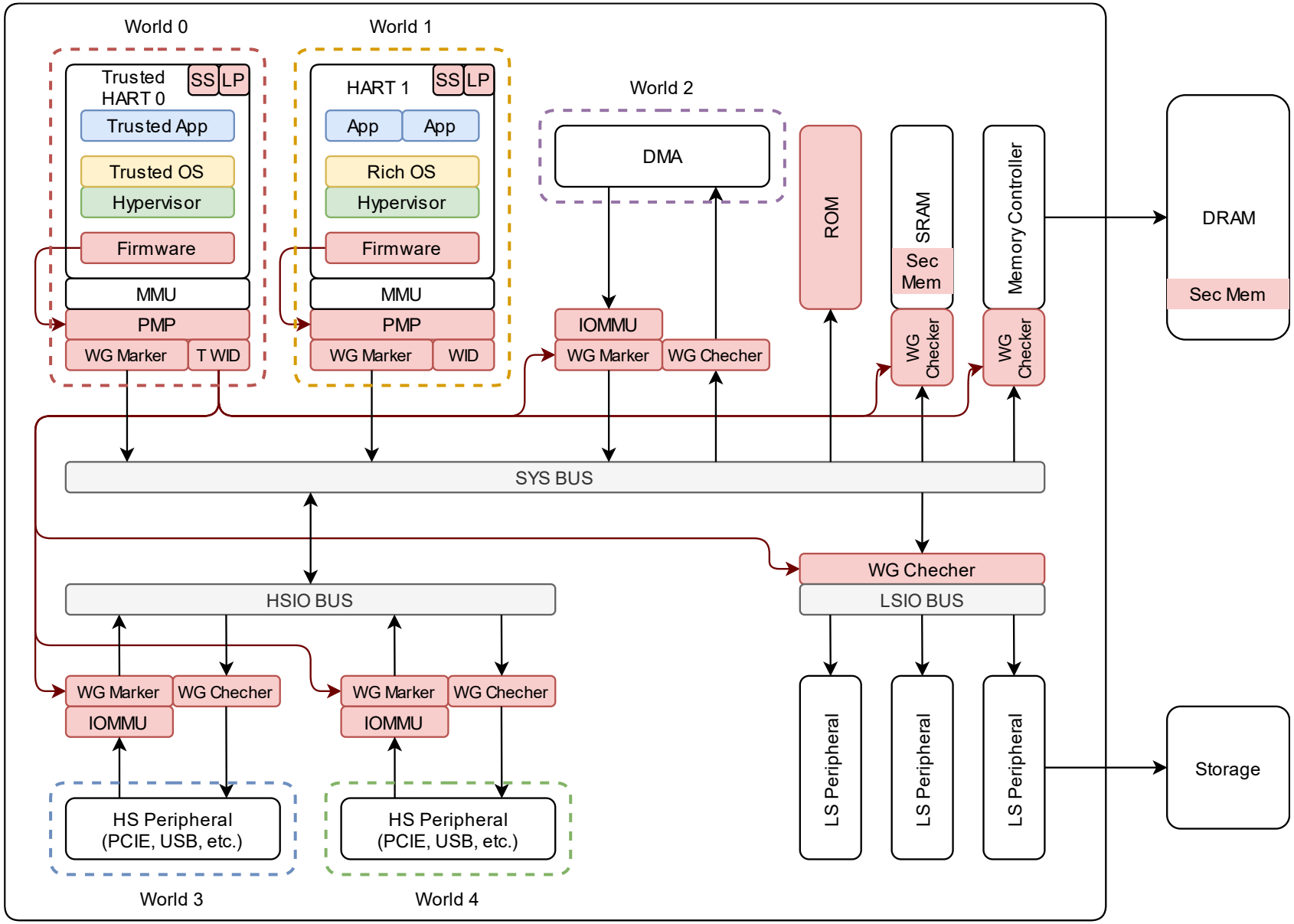
Аппаратный корень доверия в защищенном периметре

Основа надежной СДЗ

Доверенная ОС для доверенных приложений

Ограниченный функционал

SoC with WorldGuard



Гибкое управление механизмами безопасности

Подходит для реализации любого варианта ДСИ

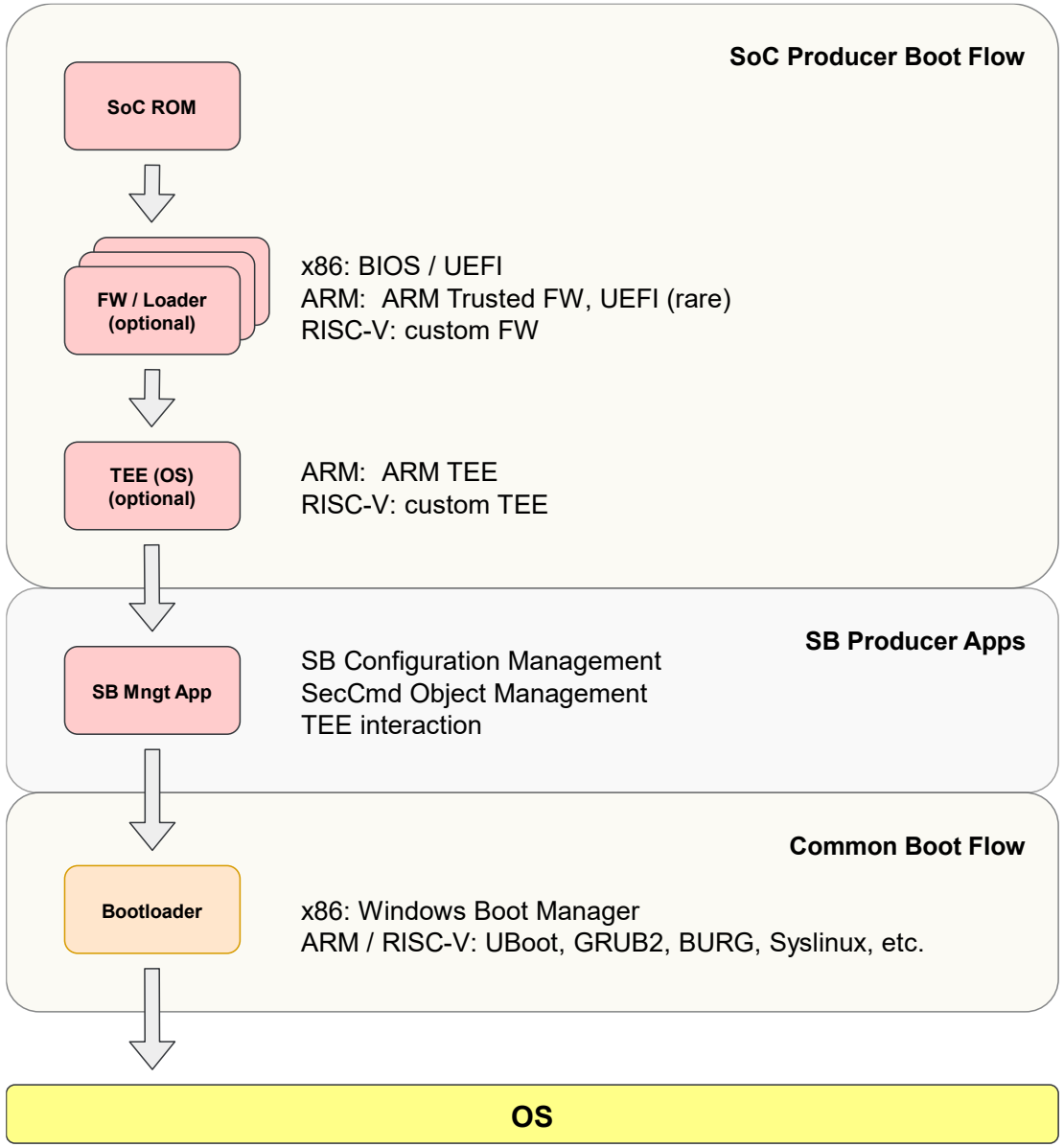
Идеально для больших систем (много памяти, периферии)

Эффективный контроль ресурсов

Аналог ARM TrustZone®

Вопросы разработки доверенного ПО для защищённых СнК

Система Доверенной Загрузки / Secure Boot



SW Vendor Assets

- Vendor ID
- Vendor Product Version
- Vendor Product Key
- Vendor Data Encryption Key
- Vendor Authentication Key

Цепь загрузки ОС на СнК с включением в нее компонентов сторонних разработчиков СДЗ

SW Vendor предоставляет индивидуальный пакет ключей для HW Vendor для поддержания уровня безопасности СДЗ и дальнейшего управления

Переданный пакет ключей хранится в защищенном хранилище и управляется ДСИ СнК

Данные принадлежащие SW Vendor хранятся в отдельной внешней микросхеме памяти

В случае невозможности использовать стороннюю часть цепи загрузки, будет работать загрузчик по умолчанию от производителя СнК

Заключение

Спасибо за внимание!

- Не доверяете? Не доверяйте! Проверяйте!
- Теория vs Практика = Документация vs Реализация
- Один в поле не воин! Безопасность – это результат коллективных усилий:

  Producer – Vendor – Deployer / Maintainer – User

- Коммуникация + Коллаборация = Результат
- Надо. Делать. Стандарты.

БУДУЩЕЕ
В НАШИХ
РУКАХ