Анализ процессора i.MX RT1060

Матвей Русаков m.rusakov@innopolis.university SD-03

Апрель 2025

1 Обзор

i.MX RT1060 - это crossover микроконтроллер от NXP на базе одного ядра Arm Cortex-M7 с тактовой частотой до 600 МГц. Он интегрирует высокопроизводительные функции, такие как 1 МБ встроенной оперативной памяти, 32 КБ кэш-памяти инструкций, 32 КБ кэш-памяти данных и блок с плавающей точкой (VFPv5). Целевая область применения - промышленные HMI, управление двигателями, бытовая техника и другие задачи, требующие производительности между классическими MCU и приложенческими процессорами.

2 Компоненты

- Ядро Arm Cortex-M7 с интегрированным MPU, поддерживающим до 16 зон защиты
- 512 КБ объединённой памяти с тесной связью для инструкций и данных (ITCM/DTCM)
- 1 МБ встроенной оперативной памяти (OCRAM)
- Различные периферийные интерфейсы: 2D графика, интерфейс камеры, контроллеры внешней памяти (SEMC, FlexSPI), аудио интерфейсы, контроллеры дисплея
- Контроллер системного сброса (SRC), защищённое энергонезависимое хранилище (SNVS)
- Контроллер одноразовой программируемой памяти (OCOTP)
- Сетевая шина (NIC-301)
- DMA контроллеры (eDMA, DMAMUX)
- Продвинутое управление питанием с DCDC и LDO регуляторами

3 Карта памяти

Карта памяти обширна, включает:

- Встроенную оперативную память (OCRAM и FlexRAM)
- Память с тесной связью (ITCM/DTCM)
- Регистры периферии, отображённые в пространствах AHB/APB

- Интерфейсы внешней памяти (FlexSPI, SEMC)
- Защищённое энергонезависимое хранилище и область OTP-фьюзов

Подробная карта памяти и описание регистров приведены в главах 2, 27, 30, 31 и других разделах руководства.

4 Механизмы безопасности включают:

- Встроенный MPU с настраиваемыми зонами защиты памяти
- Защищённое энергонезависимое хранилище (SNVS) для безопасного хранения ключей и обнаружения взлома
- Одноразовые программируемые фьюзы (OTP) для конфигурации загрузки и настроек безопасности
- Контроллер системного сброса для управления безопасными последовательностями сброса
- Защита доступа в мостах шины (AIPSTZ) для ограничения несанкционированного доступа к периферии и памяти
- Конфигурация загрузки через фьюзовую карту, управляющую безопасной загрузкой и блокировкой устройства

Эти механизмы направлены на предотвращение неавторизованного выполнения кода, защиту конфиденциальных данных и обеспечение безопасной загрузки.

5 Процесс загрузки

Процесс загрузки гибко настраивается через фьюзы:

- Загрузка из внутренней или внешней памяти (FlexSPI, SEMC)
- Безопасная загрузка с проверкой подлинности образов с помощью ключей из OTP/SNVS
- Фьюзовая карта задаёт выбор загрузочного устройства, параметры безопасности и статус блокировки
- Контроллер OTP управляет программированием и блокировкой фьюзов

Загрузчик проверяет целостность и подлинность образа перед запуском, используя аппаратные модули безопасности.

6 Выводы и наблюдения по безопасности

i.MX RT1060 сочетает высокую производительность с продвинутыми средствами безопасности, подходящими для встроенных систем с повышенными требованиями. Потенциальные риски безопасности:

- Очень важно правильно настроить MPU и контролировать доступ, чтобы избежать повышения привилегий

- Безопасная загрузка зависит от корректного программирования OTP-фьюзов; ошибки ослабляют защиту
- Физические атаки на области OTP и SNVS требуют учёта в модели угроз
- Необходимо включать и настраивать защиту шины и периферии для предотвращения несанкционированного доступа

В целом, устройство предоставляет надёжную платформу для безопасных систем, однако безопасность сильно зависит от правильной конфигурации и процессов безопасного программирования.

References

[1] i.MX RT1060 Processor Reference Manual, Document Number: IMXRT1060RM Rev. 3, 07/2021

[2] GitHub Link: https://github.com/MattWay224/reverse-engineering-course