

Исследование методов горячего обновления ПО для ОСРВ с переиспользованием состояния программы

Иван Солодовников

Научный руководитель:
Виталий Чепцов, ИСП РАН

17 марта 2025 г.

Содержание

1 Введение

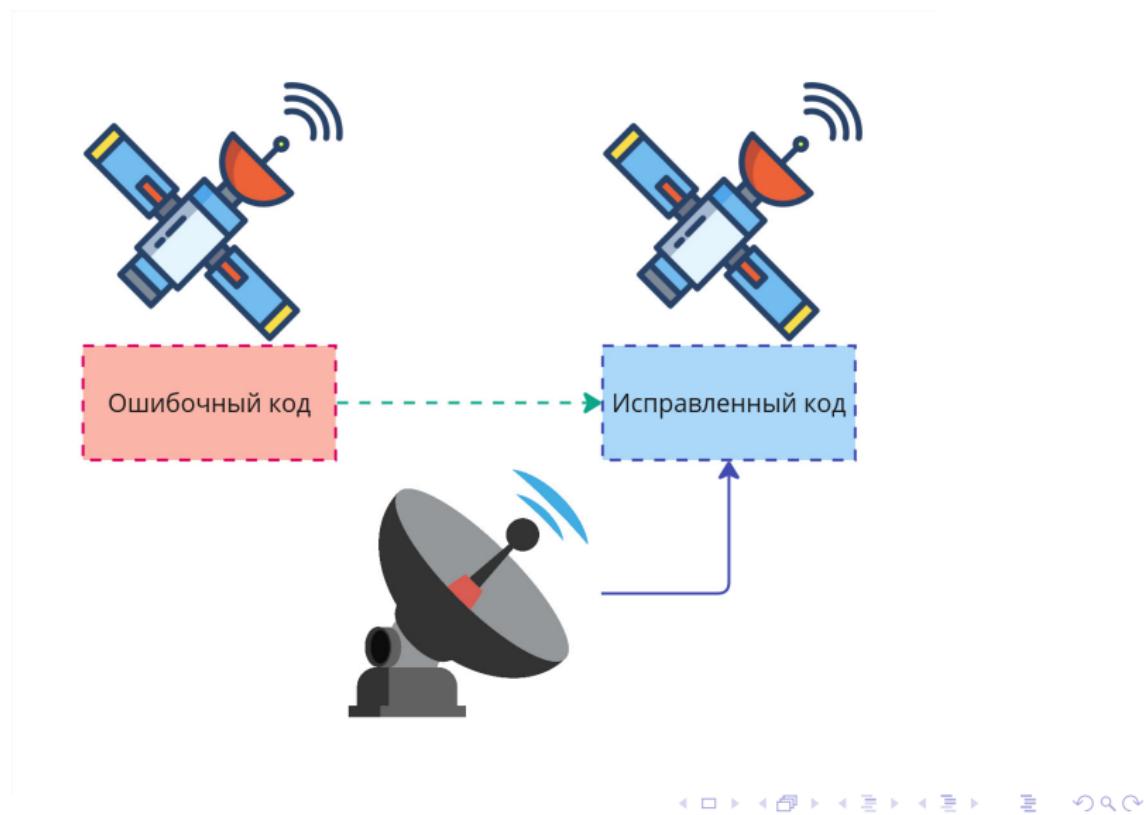
2 Исследование

3 Проделанная работа

Основные определения

- **Операционная система реального времени (OCPB, RTOS)** — операционная система, предназначенная для исполнения задач с заданными ограничениями на время исполнения.
- **ARINC 653** — спецификация OCPB, применяемых в авионике.
- **Раздел (партиция, partition)** — единица планирования в ARINC 653.
- **Горячее обновление (hotpatching, livepatching)** — обновление, применяемое к исполняемому коду в процессе его работы.

Постановка проблемы



Цель исследования

Цель — поиск метода формирования и применения обновления исполняемого кода раздела ОСРВ.

Задачи:

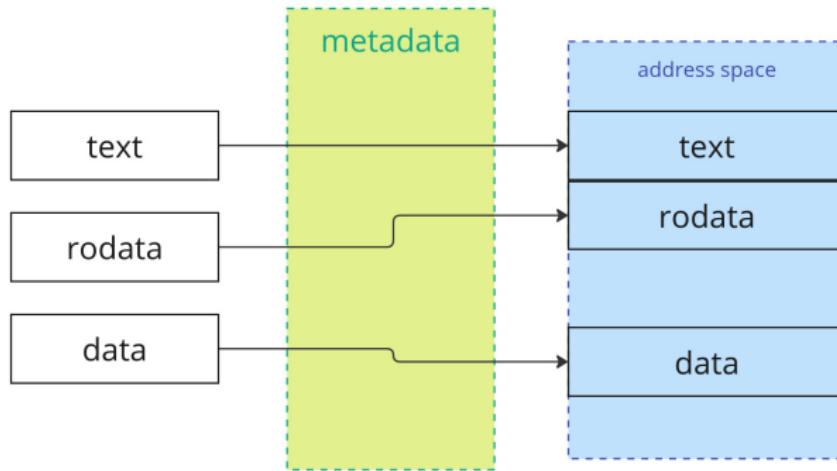
- Исследовать имеющиеся подходы к горячим обновлениям ПО;
- Спроектировать архитектуру, позволяющую применять горячие обновления различного объёма:
 - 1 Обновление кода раздела целиком,
 - 2 Обновление используемой системной библиотеки,
 - 3 Обновление одной из функций в коде раздела;
- Разработать прототип, демонстрирующий возможности горячих обновлений.

Имеющиеся решения

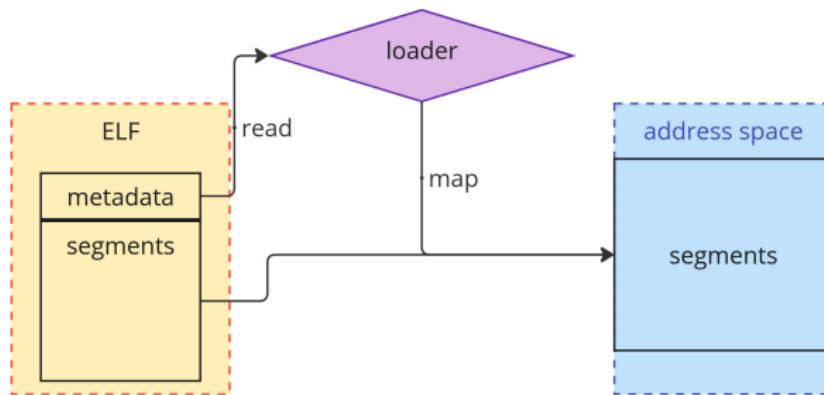
- Linux
 - ksplice[1] – Oracle
 - kpatch – RedHat
 - kGraft – SUSE
- ОСРВ для IoT
 - HERA[2] – только для процессоров ARM



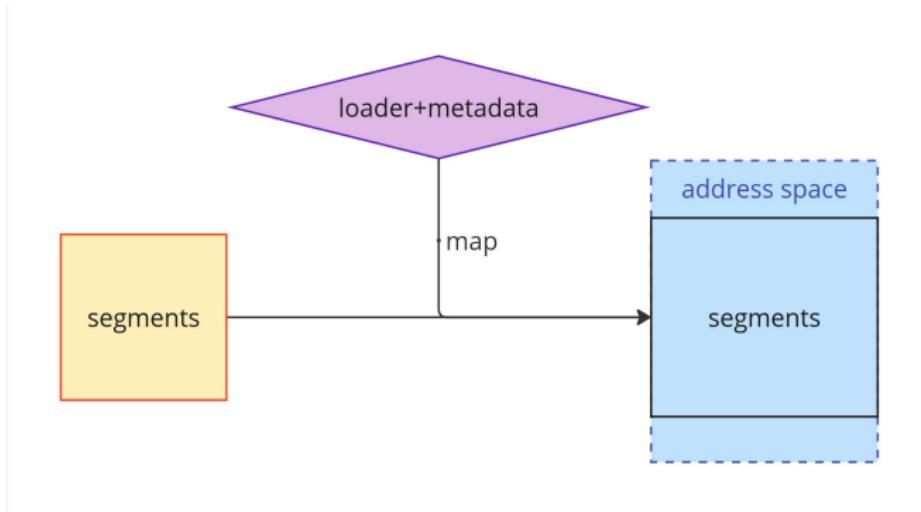
Работа загрузчика



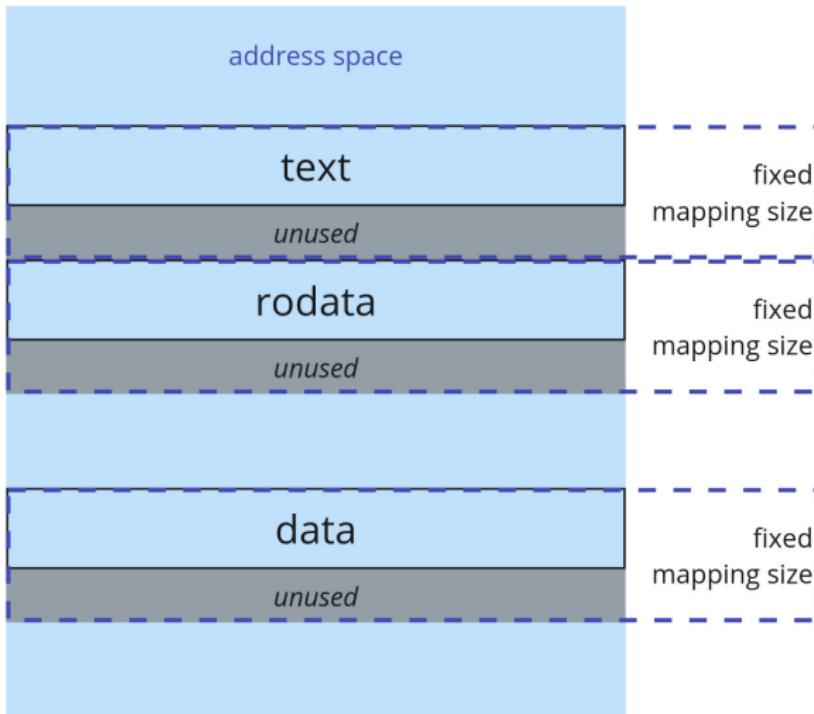
Загрузчик Linux



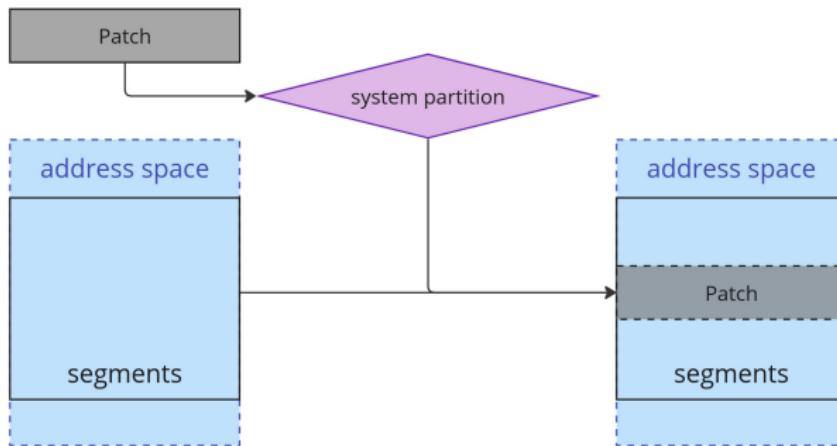
Загрузчик ОСРВ



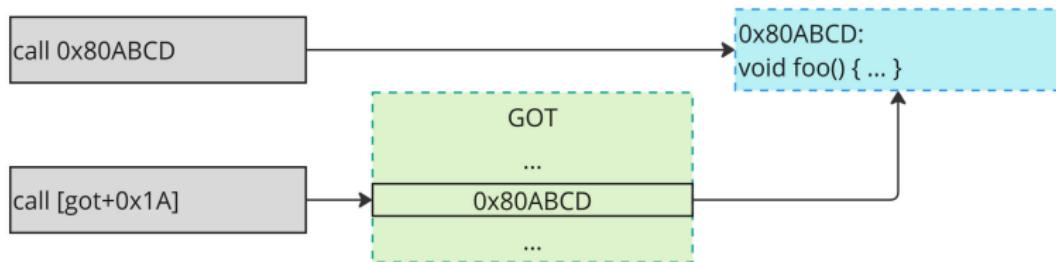
Фиксированная раскладка памяти



Особенности обновления



Динамическое связывание



Промежуточные итоги

- Произведён обзор ряда имеющихся подходов к горячему обновлению.
- Решена проблема обновления в условиях неизменной раскладки памяти. Фиксация размеров отображений сегментов в виртуальную память позволяет производить горячие обновления с полной заменой кода раздела.

Следующие шаги

- Продолжить рассмотрение созданных подходов к горячему обновлению. Особенное внимание следует уделить исследованиям, касающимся обновления приложений для ARINC-653-совместимых ОСРВ.
- Исследовать возможность использования идеи динамического связывания для обновления кода системных библиотек.

Список литературы

- [1] J. Arnold и M. F. Kaashoek, «Ksplice: Automatic rebootless kernel updates,» в *Proceedings of the 4th ACM European conference on Computer systems*, 2009, с. 187—198.
- [2] C. Niesler, S. Surminski и L. Davi, «HERA: Hotpatching of Embedded Real-time Applications.,» в *NDSS*, 2021.