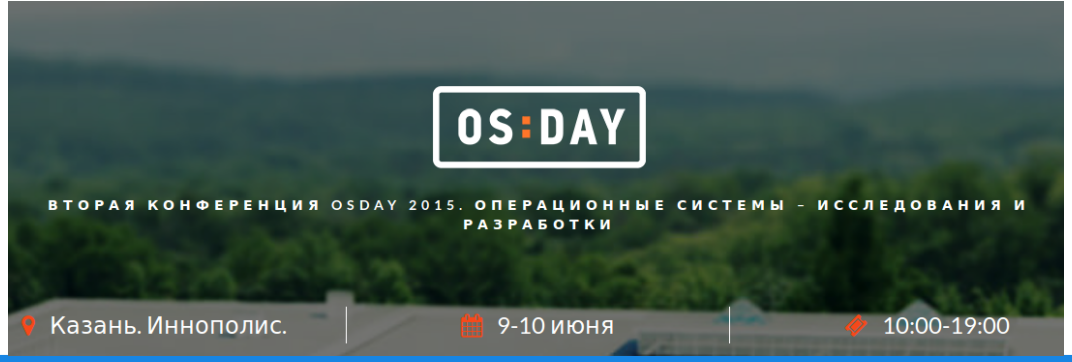


Российские операционные системы реального времени

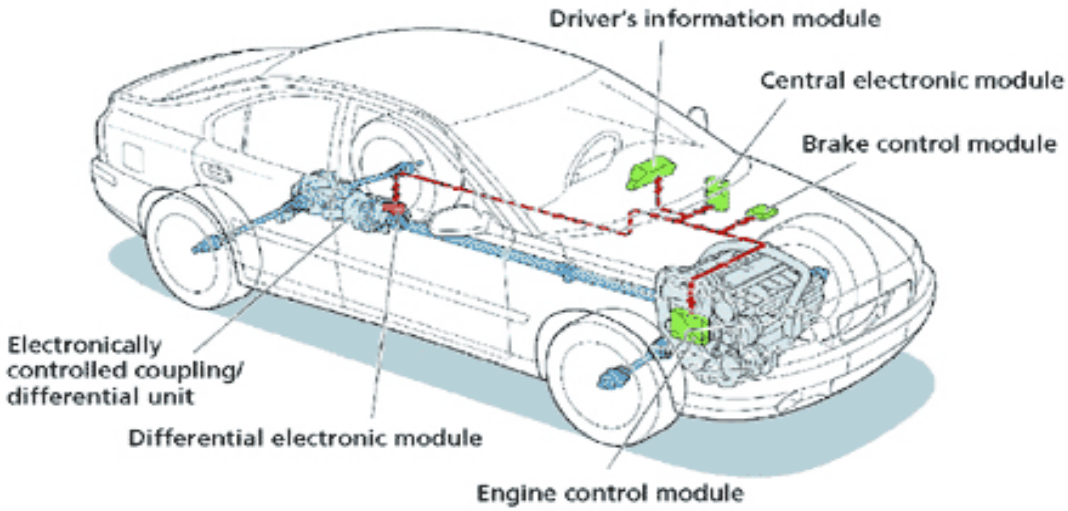
Алексей Хорошилов

ИСП РАН

Институт системного программирования РАН

Операционные системы реального времени

- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами



Операционные системы реального времени

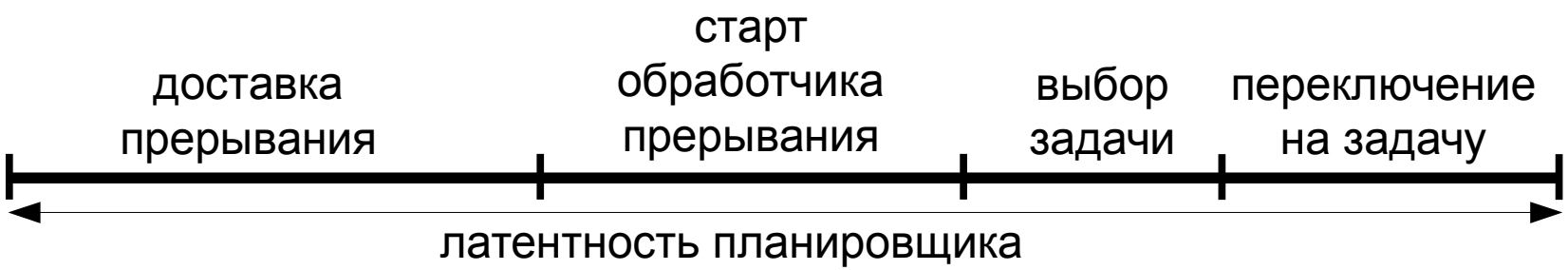
- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами
- особенности
  - **детерминизм**

Детерминизм

- Детерминизм по времени (латентность)

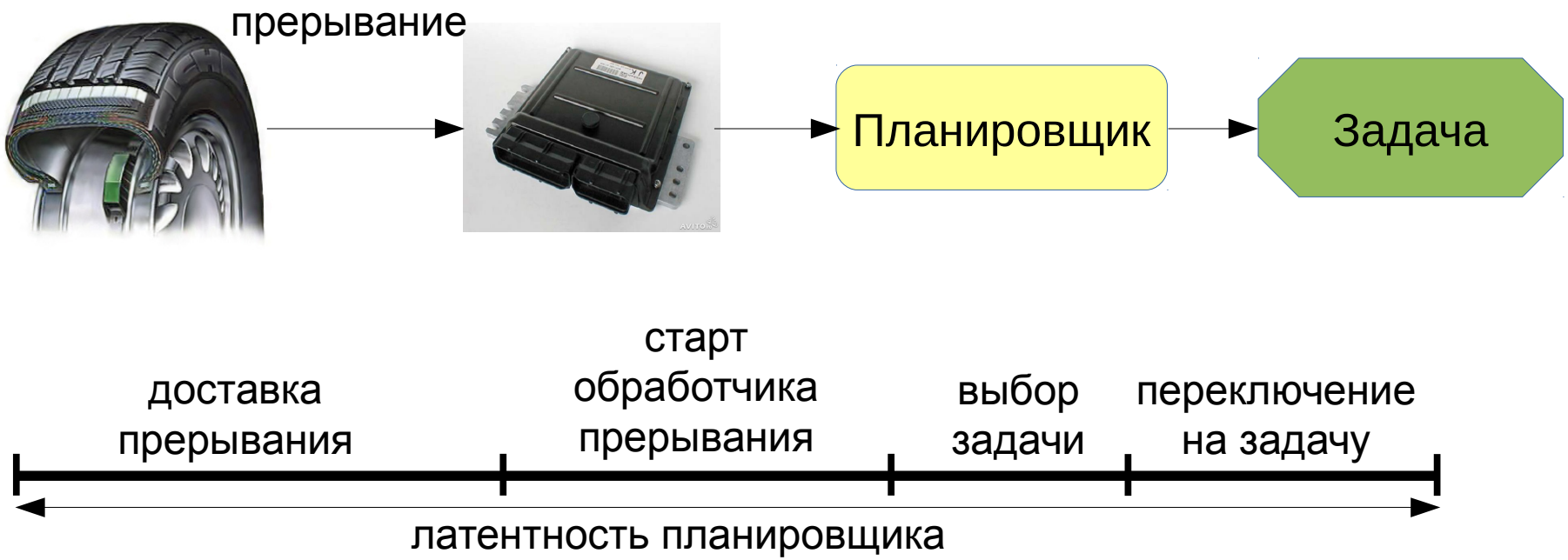
Детерминизм

- Детерминизм по времени (латентность)

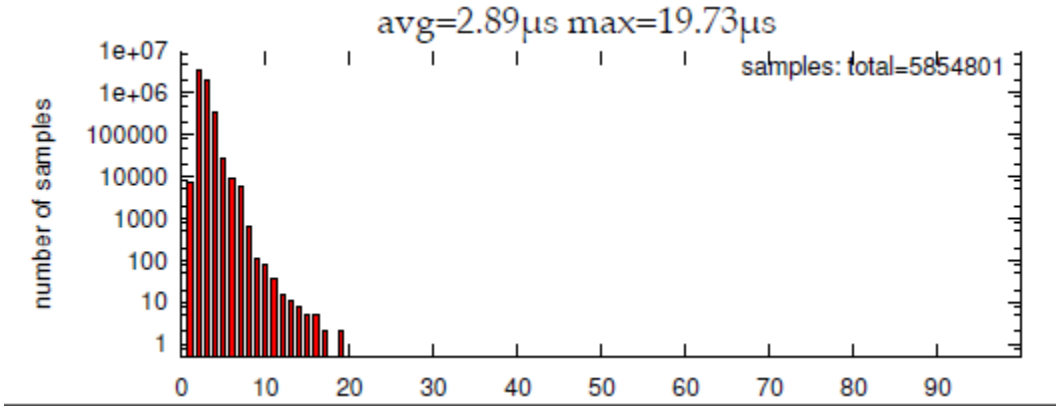


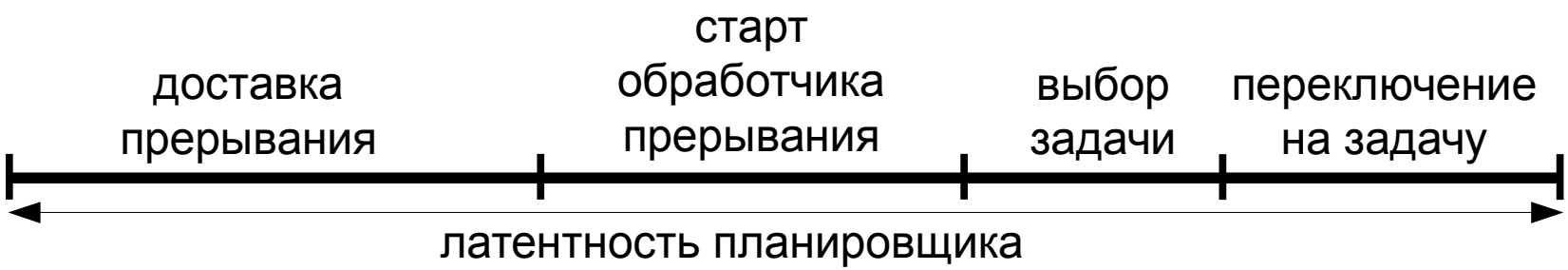
Детерминизм

- Детерминизм по времени (латентность)



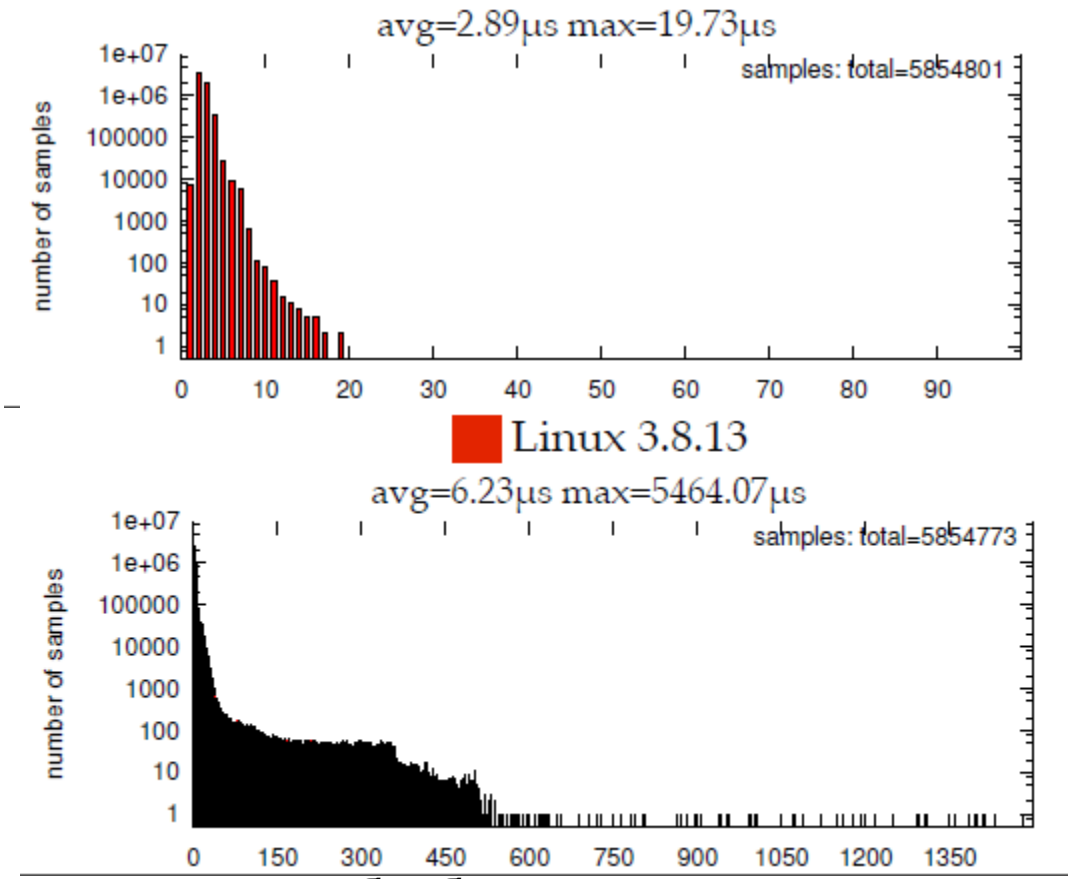
Латентность обычной ОС





(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Латентность обычной ОС

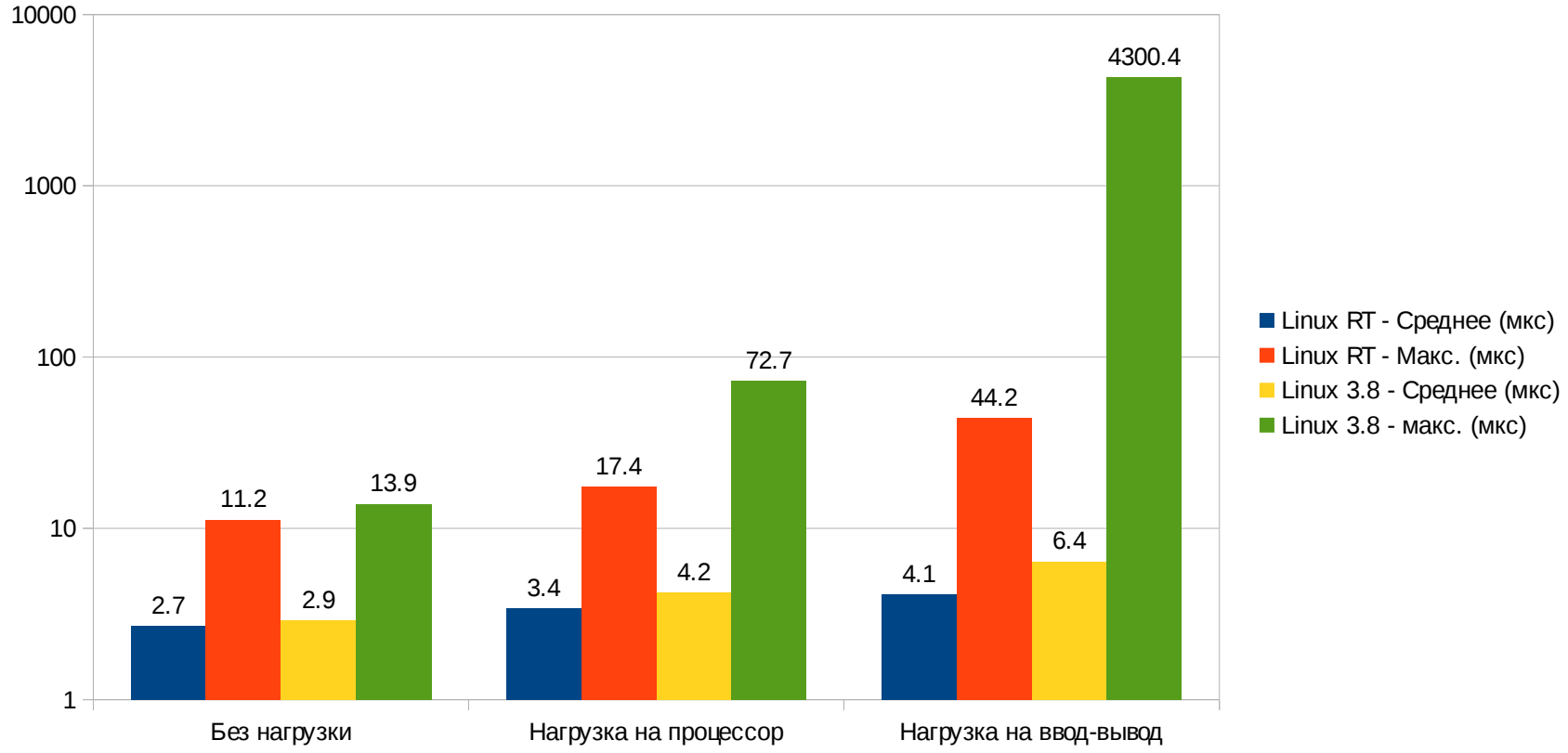


доставка прерывания | обработчика прерывания | выбор задачи | переключение на задачу

латентность планировщика

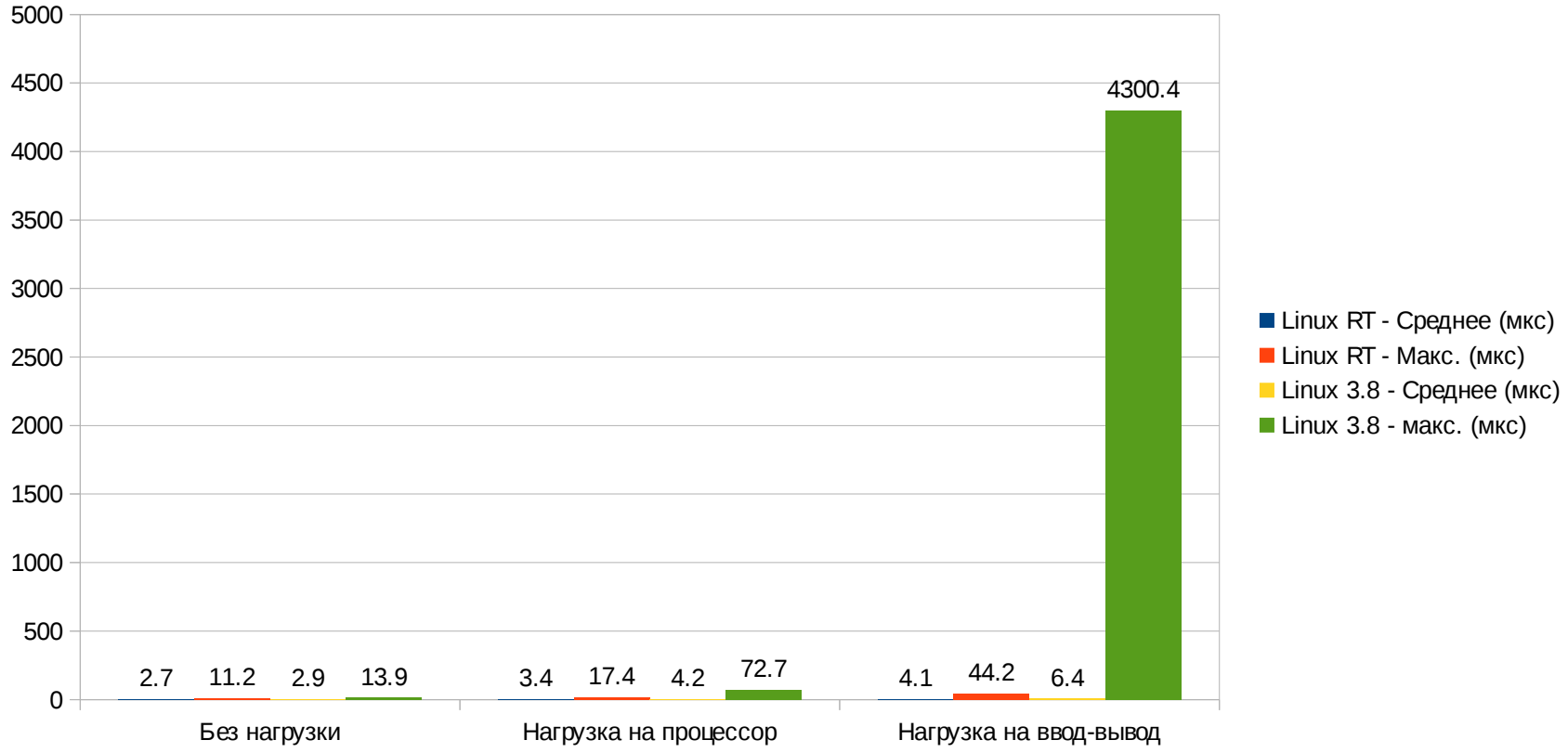
(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Linux-RT



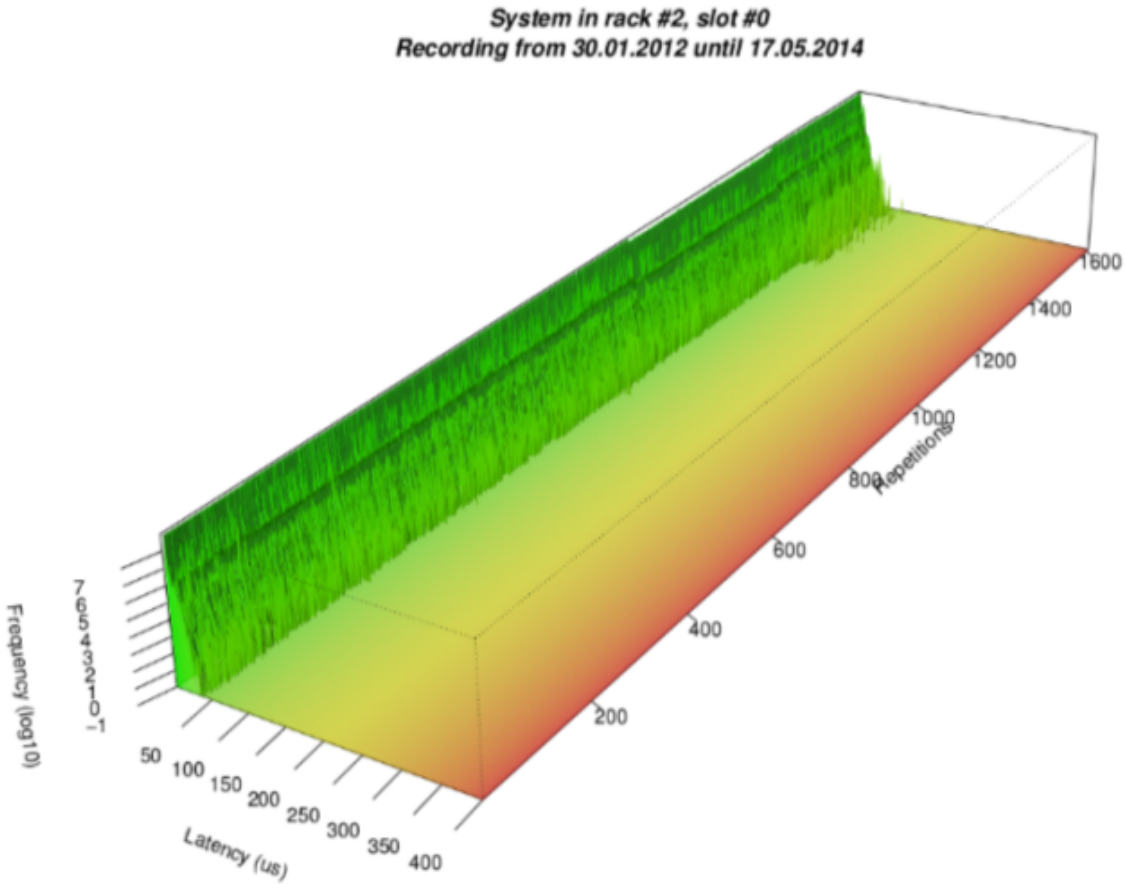
(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Linux-RT



(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Assurance Data - OSADL QA-Farm



Long term measurements under specified conditions - http://www.osadl.org/QA

Операционные системы реального времени

- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами
- особенности
  - детерминизм
  - **ограниченные ресурсы**

Ограниченные ресурсы

- 4 Мб оперативной памяти
- Процессоры со встроенной памятью
    - SRAM (< 1024kB)
    - например, Intel Quark - 512 Kb
- Процессоры без MMU

Ограниченные ресурсы и Linux

- Linux-3.17-rc1 (x86)

make defconfig	16532k
make allnoconfig	1269k
make tinyconfig	1048k
+ ELF support	+4k
+ modules	+53k
+ initramfs	+37k
+ flash storage	…
+ filesystem	
+ networking	

Операционные системы реального времени

- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами
- особенности
  - детерминизм
  - ограниченные ресурсы
  - **специфический набор сервисов**

Специфичный набор сервисов

- ARINC-653 API
- Статическое распределение ресурсов
  - Статическая циклограмма на уровне разделов (partitions)
  - Статическое распределение памяти
  - Общение между разделами только посредством каналов

Операционные системы реального времени

- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами
- особенности
  - детерминизм
  - ограниченные ресурсы
  - специфический набор сервисов
  - **сертификация**

Сертификация

- Ответственное применение

Сертификация

- **DO-178B** Software considerations in Airborne Systems and Equipment Certification
- **IEC 60880(2006)** Nuclear power plants – Instrumentation and control systems important to safety
- **МАК КТ-178В** Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники
- **ГОСТ РВ 0019-001** Программное обеспечение встроенных систем
- ...

Категории отказных ситуаций

- Категория A – Катастрофическая
  - Препятствует безопасному функционированию объекта управления
- Категория B – Опасная / критическая
  - Приводит к критическому уменьшению возможностей объекта управления или способности персонала справиться с неблагоприятными режимами
- Категория C – Существенная
  - Приводит к существенному снижению возможностей объекта управления или способности персонала справиться с неблагоприятными режимами
- Категория D – Несущественная
  - Незначительно уменьшает безопасность объекта и требует действий персонала, которые осуществимы в пределах их возможностей

Сертификационные данные (DO-178B)

- План сертификации
- Архитектура
- Требования
- Оценка функциональных рисков
- Оценка безопасности системы
- Анализ общих причин отказов
- Данные валидации
- Данные верификации
- Указатель конфигурации
- …

до 18 видов документов

FINMECCANICA LINUX

FINMECCANICA

FINMECCANICA LINUX

Create a common reference Linux distribution that Satisfy all FNM companies' needs in a single product:

- Hard Real Time on multi-core CPU
- Scalability (from embedded –avionics- to workshop –networking-)
- Architecture heterogeneity (x86, PPC, ARM, Cell,…)
- Safety (DO178B, ARINC 653, IEC 61508,…)

Reduce dependence on a product, less risk for "locking in" effects overall Lower costs
Increase quality and stability
In house Know-how development

AnsaldoBreda
Una Società Finmeccanica

ELSAG DATAMAT
Finmeccanica

SELEX GALILEO

MBDA
MISSILE SYSTEMS

SELEX
Sistemi Integrati
A Finmeccanica Company

AleniaSIA
A Finmeccanica Company

TELESPAZIO
A Finmeccanica / Thales Company

DO-178B

RTCA

EuroTech
A MEMBER OF EUROTECH GROUP

Finmeccanica Linux

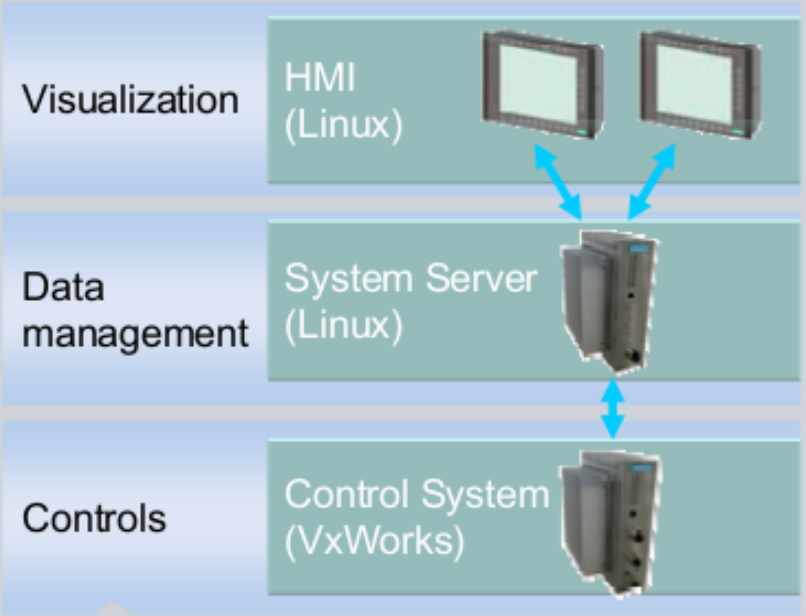
- The context was the development of a European research project which aims to deliver **a new generation Unmanned Combat Air Vehicle**. FINX-RTOS (a Gentoo based distribution managed by Finmeccanica) have been customised to satisfy Design Assurance Level D requirements. Like other Linux, FINX is “open source” so its source code was available for the reverse engineering operations needed for DO-178B certification at level D as "software previously developed". Moreover such Linux OS guarantees real-time performance needed (PREEMPT_RT patch applied) and was quite easy to realize a safety “all in RAM” operating system.
- To make a long story short, on April 2012 FIN.X-RTOS was declared compliant after the last Stage Of Involvement meeting: “The Software Review 4 (SR4) audit for the FIN.X-RTOS CSCI ensures that final compliance to all the **DO-178B level D** objectives has been achieved and all open items have been addressed.” as stated by the Technical Quality.

Project context: Linux-based vehicle control system

SIEMENS

Sibas PN: Siemens Mobility's new generation of vehicle control systems

- Release begin 2011
- Lower costs via platforms like Simatic and Linux
- Based on industry standards



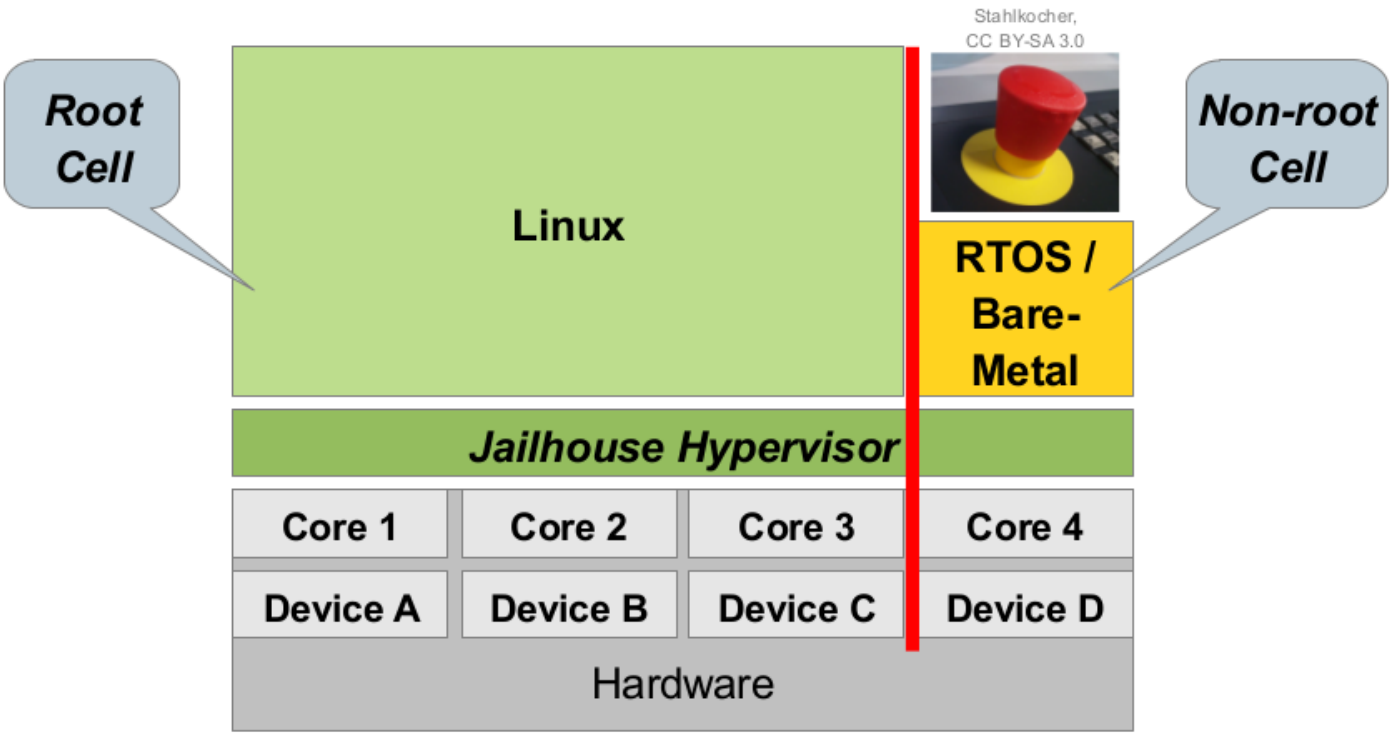
General requirements:

- **Linux** used on some components to fulfill **technical** and **commercial requirements**
- Functionality up to **safety integrity level (SIL) 2**

→How is Linux correctly handled within this safety-related system?

© Siemens AG, Corporate Technology

Гипервизор Siemens Jailhouse

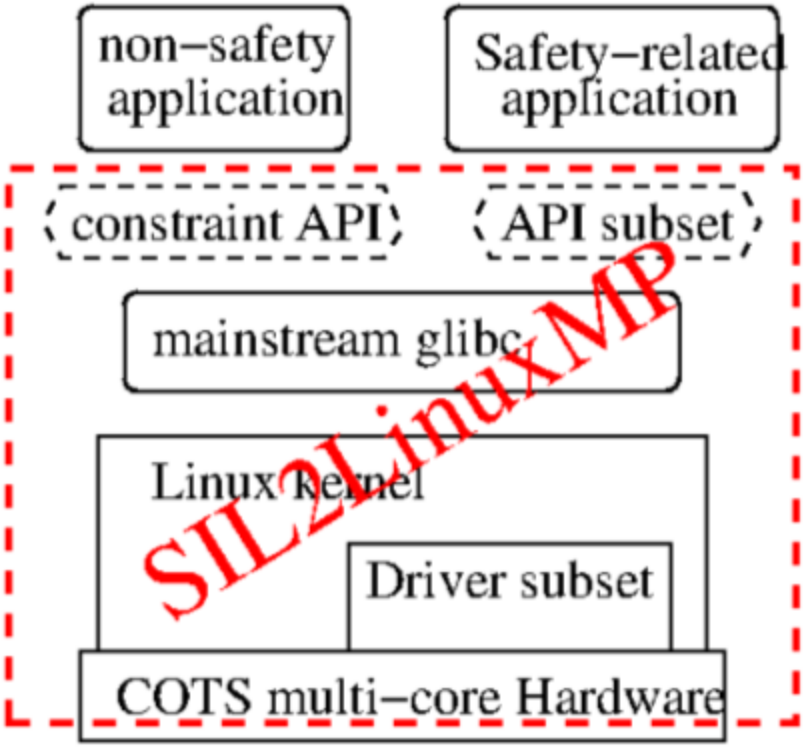


Linux или не Linux?

Linux или не Linux?

+ мягкое реальное время
+ широкая функциональность
+ поддержка оборудования
- размер кода
- скорость развития
- исходный дизайн и развитие без учёта требований по безопасности

Linux или не Linux?



Оценка трудоёмкости разработки

	Кол-во приложений	Аппаратные устройства	Трудоёмкость чел.лет
ОС общего назначения			~100 000
Десктопные ОС	~100 000	~10 000	
Мобильные ОС	~100 000	~10 000	
Серверные ОС	~10 000	~10 000	
Суперкомпьютерные ОС	~1 000	~100	
Встраиваемые ОС			
ОС реального времени	~1 000	~10	~10-100
Встраиваемые ОС с интерфейсом	~10 000	~100	~1 000
Гипервизоры	-	~1 000	~100-1 000
Облачные ОС	~10 000	~10	~100-1 000

Отечественные ОС РВ

	API	Архитектуры	Лицензия
ОС3000(НИИСИ РАН)	ARINC-653, POSIX	MIPS	коммерч.
ЭОС (ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» имени П. А. Ефимова»)	ARINC-653	MIPS, ARM	коммерч.
RelMK-653 (ОАО «Раменское приборостроительное конструкторское бюро»)	ARINC-653	x86, ARM	коммерч.
МОС-ОП (АО «Авиаавтоматика» имени В.В. Тарасова»)	ARINC-653, POSIX	x86, ARM, MIPS	коммерч.
Embox («Ланит-терком», СпбГУ)	POSIX	X86, ARM, Microblaze	BSD
РОК (ParisTech, ИСП РАН)	ARINC-653	x86, PPC	GPLv3
ОС «Лаборатории Касперского»	?	?	коммерч.

ОС РВ – это не только ядро

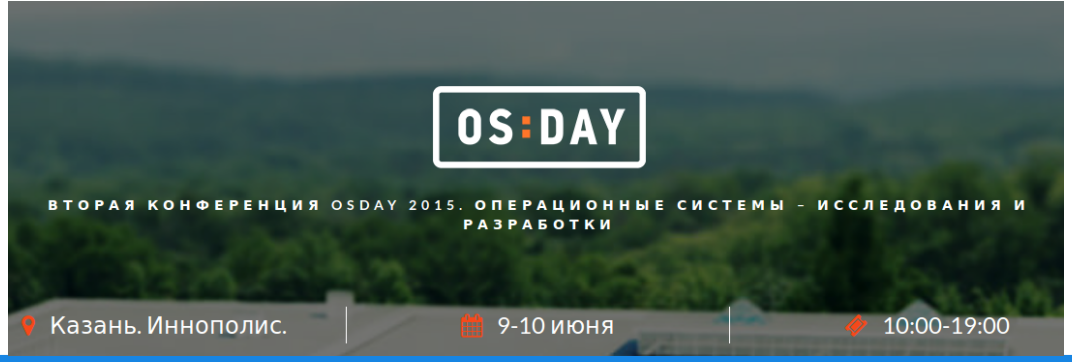
- Документация
- Компилятор
- Среда разработки
- Отладчик
- Трассировщик
- Система сборки и верификации конфигурации
- Система тестирования

Возможности для кооперации

- Общая дискуссия
  - Сегодня 14:30-16:00

Среды разработки на основе Eclipse

- Monta Vista DevRocket IDE
- Wind River Workbench
- LynuxWorks Luminosity
- Freescale CodeWarrior
- QNX Momentics
- Mentor Graphics EDGE
- Xilinx Platform Studio
- Enea Optima
- Cisco UCVP Studio
- TimeSys TimeStorm IDE



Спасибо!

Алексей Хорошилов
khoroshilov@ispras.ru

ИСП РАН
Институт системного программирования РАН