LinuxTesting.org

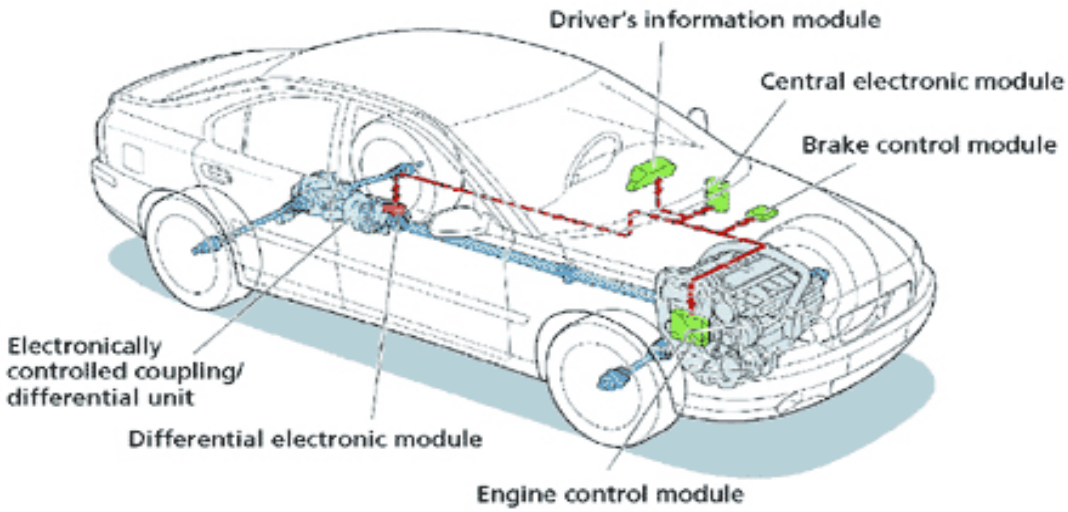
Свободная реализация ARINC-653-совместимой ОС реального времени

Николай Пакулин
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

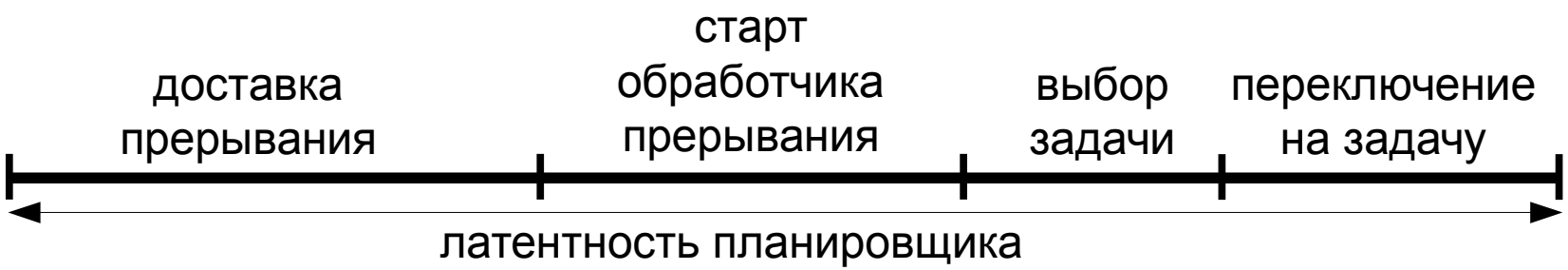
- применяются в ЭВМ, предназначенных для управление какими-либо процессами или механизмами
- особенности
  - **детерминизм**

Детерминизм

- Детерминизм по времени (латентность)

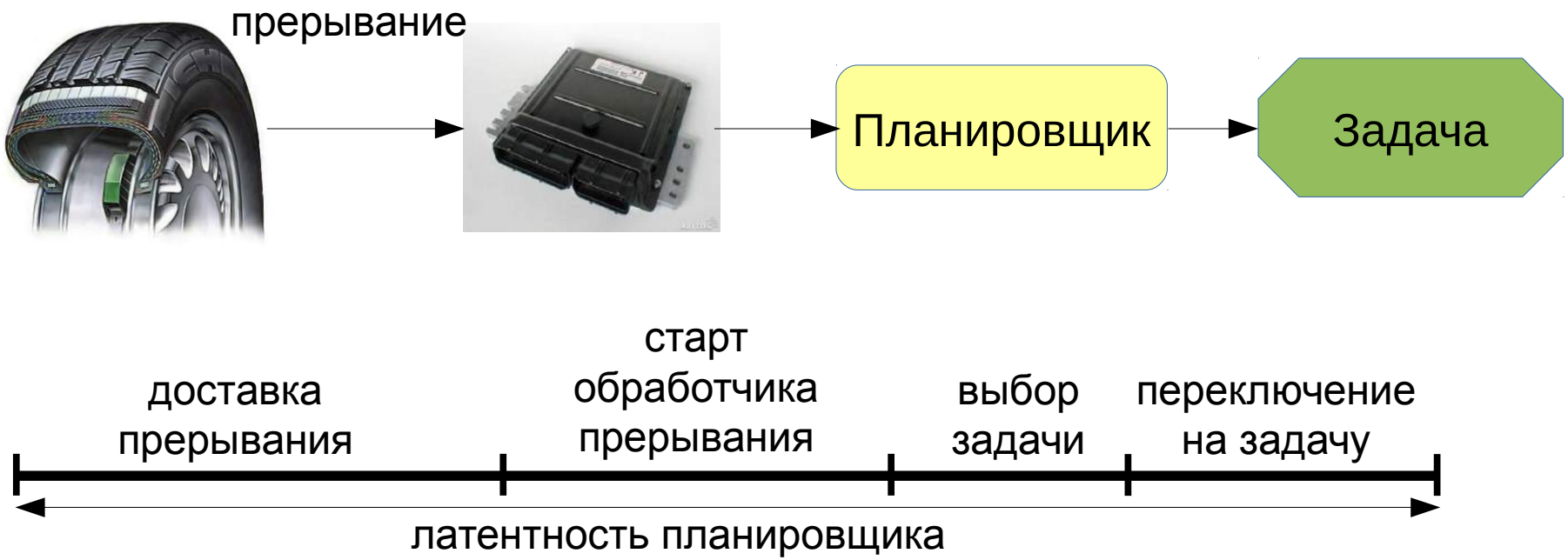
Детерминизм

- Детерминизм по времени (латентность)

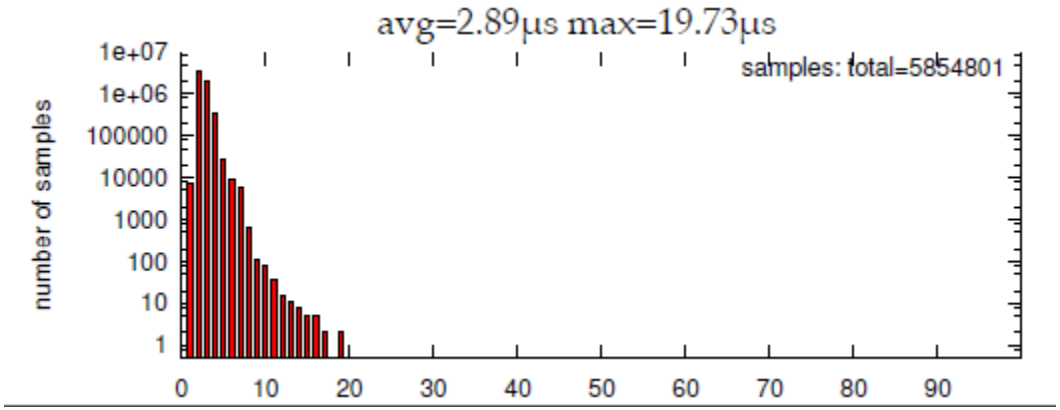


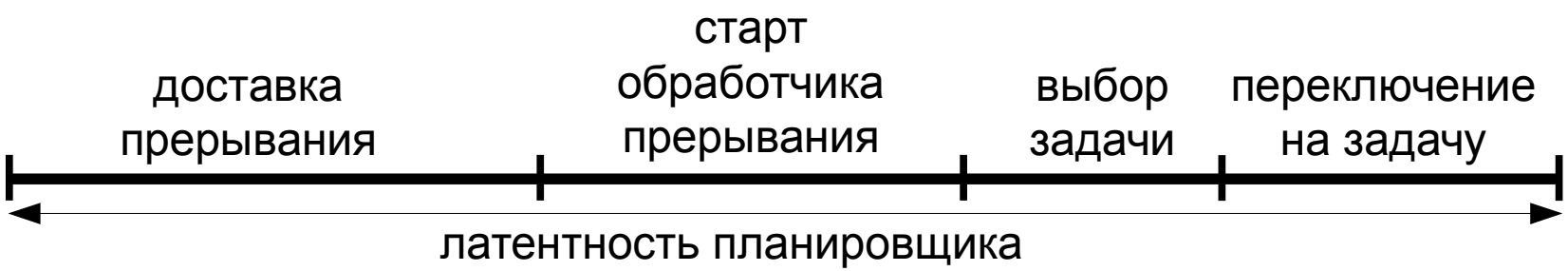
Детерминизм

- Детерминизм по времени (латентность)



Латентность обычной ОС

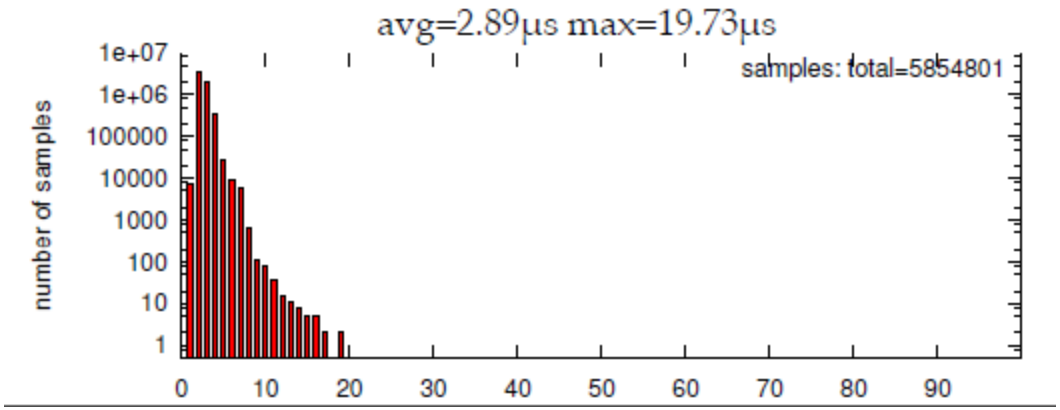




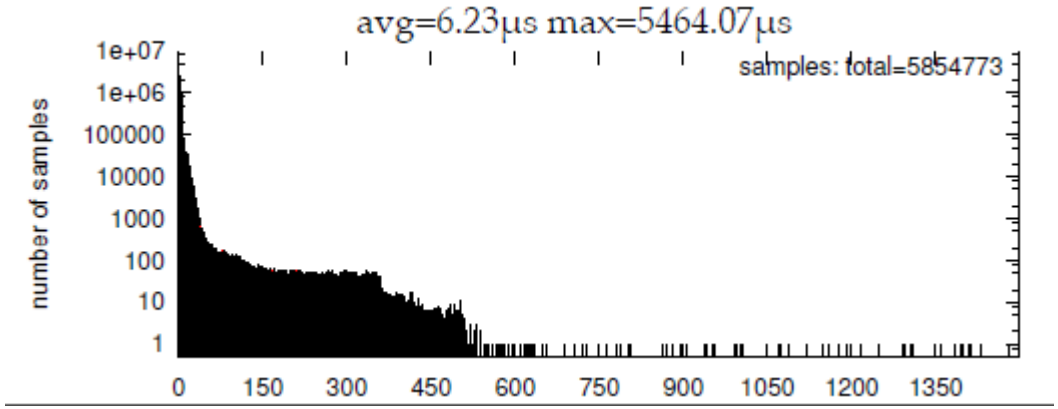
(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Латентность обычной ОС

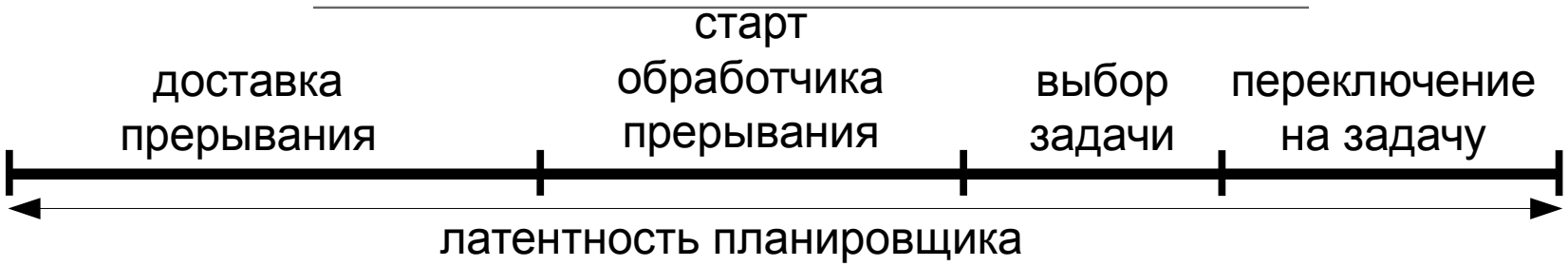
Linux 3.8.13



без нагрузки

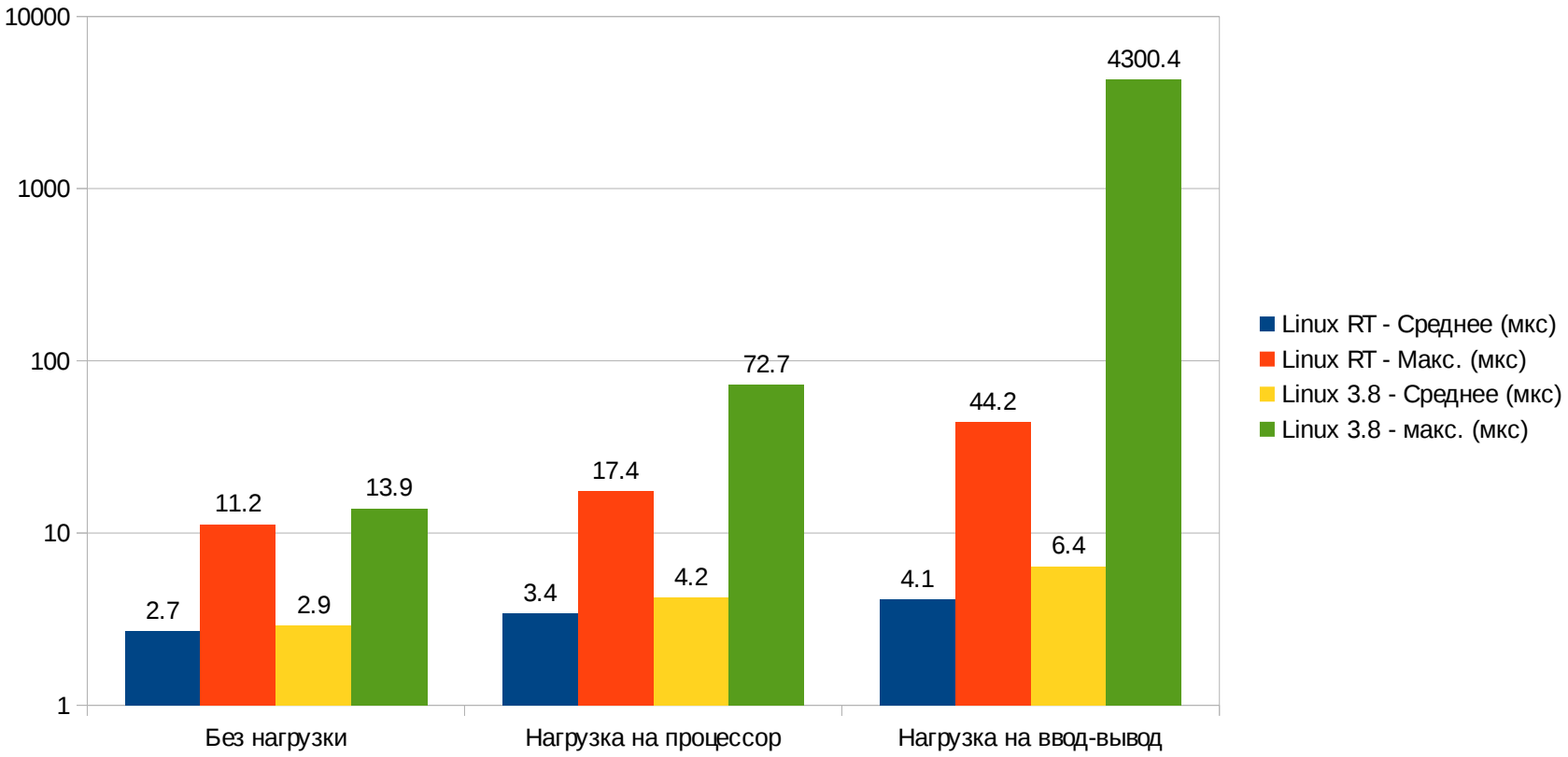


нагрузка на ввод-вывод



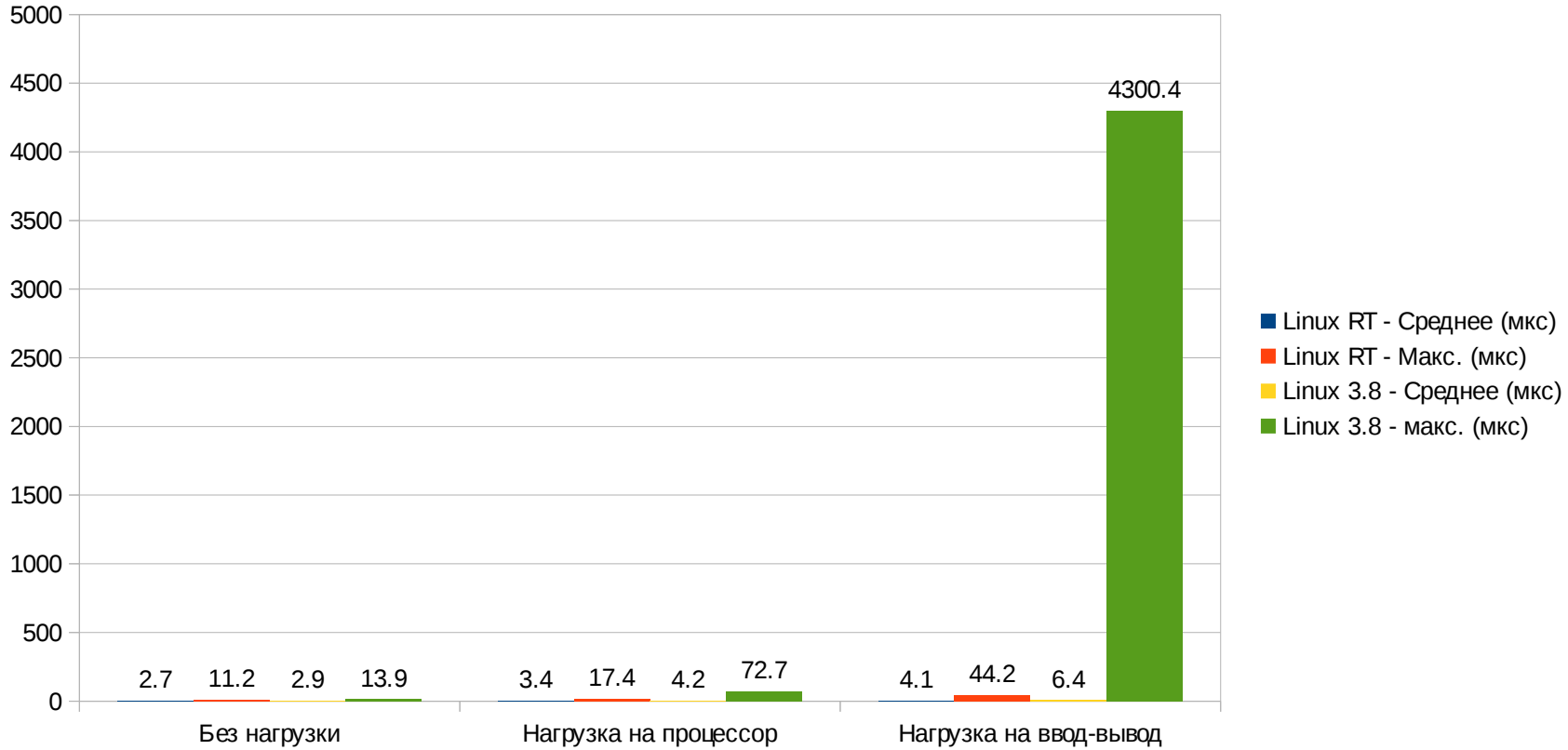
(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

Linux-RT



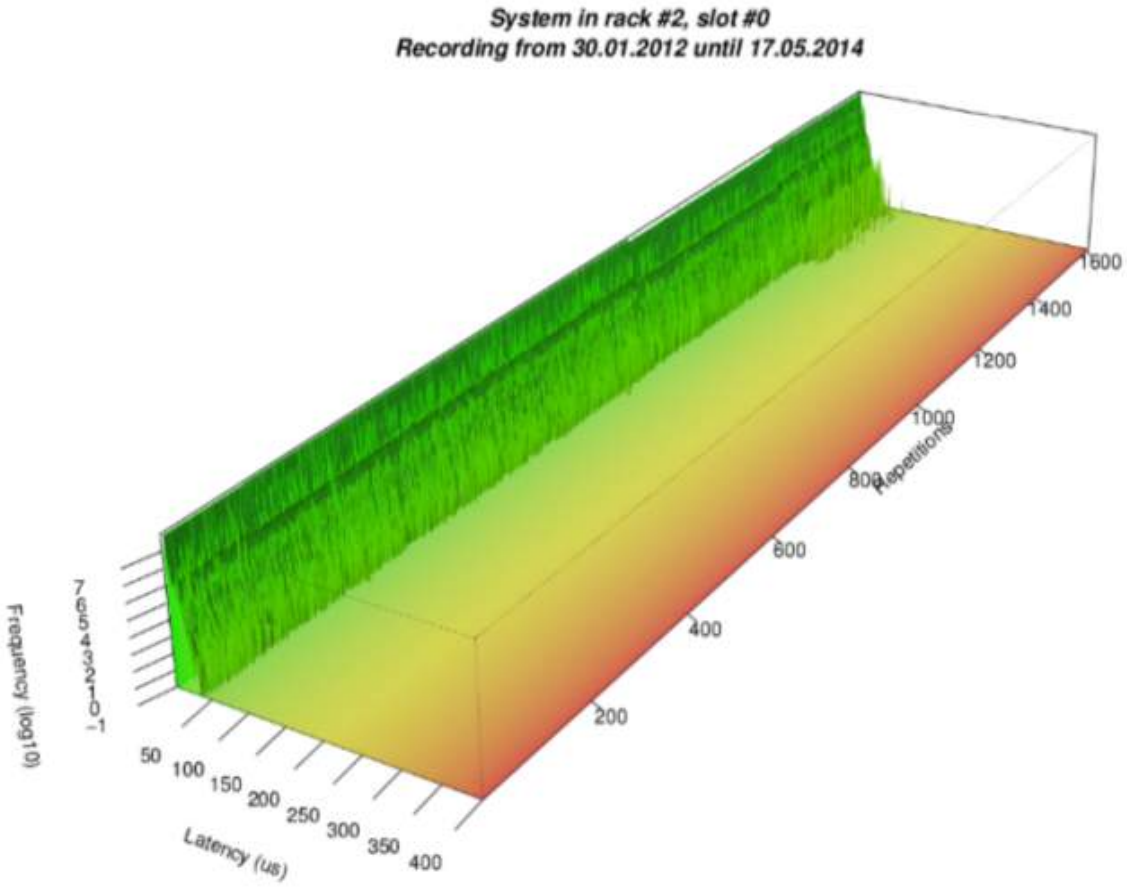
(*) F. Cerqueira and B. Brandenburg, "A Comparison of Scheduling Latency in Linux, PREEMPT-RT, and LITMUSRT"

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
  - Выделение ресурсов только на этапе инициализации
- Общение между разделами только посредством каналов
- Специфический механизм обработки ошибок (Health Monitoring)

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

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.

Категории отказных ситуаций

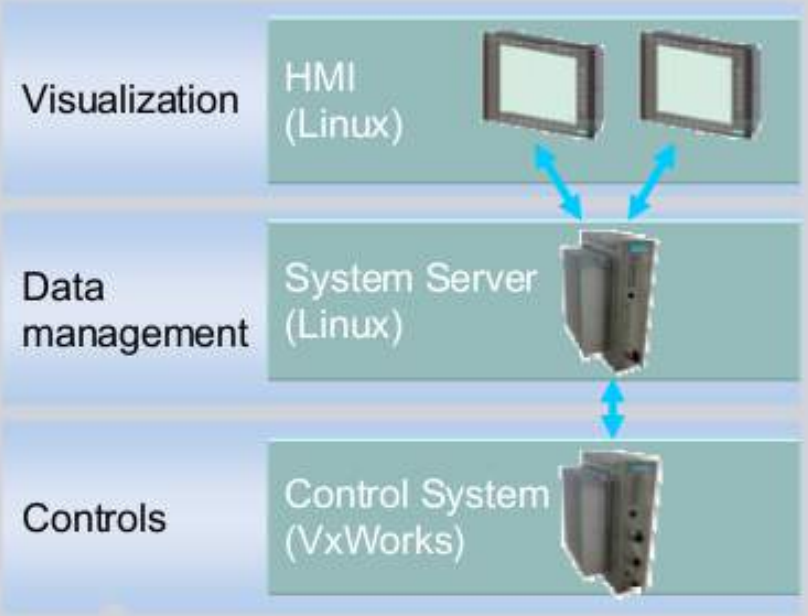
- Категория A – Катастрофическая
  - Препятствует безопасному функционированию объекта управления
- Категория B – Опасная / критическая
  - Приводит к критическому уменьшению возможностей объекта управления или способности персонала справиться с неблагоприятными режимами
- Категория C – Существенная
  - 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

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

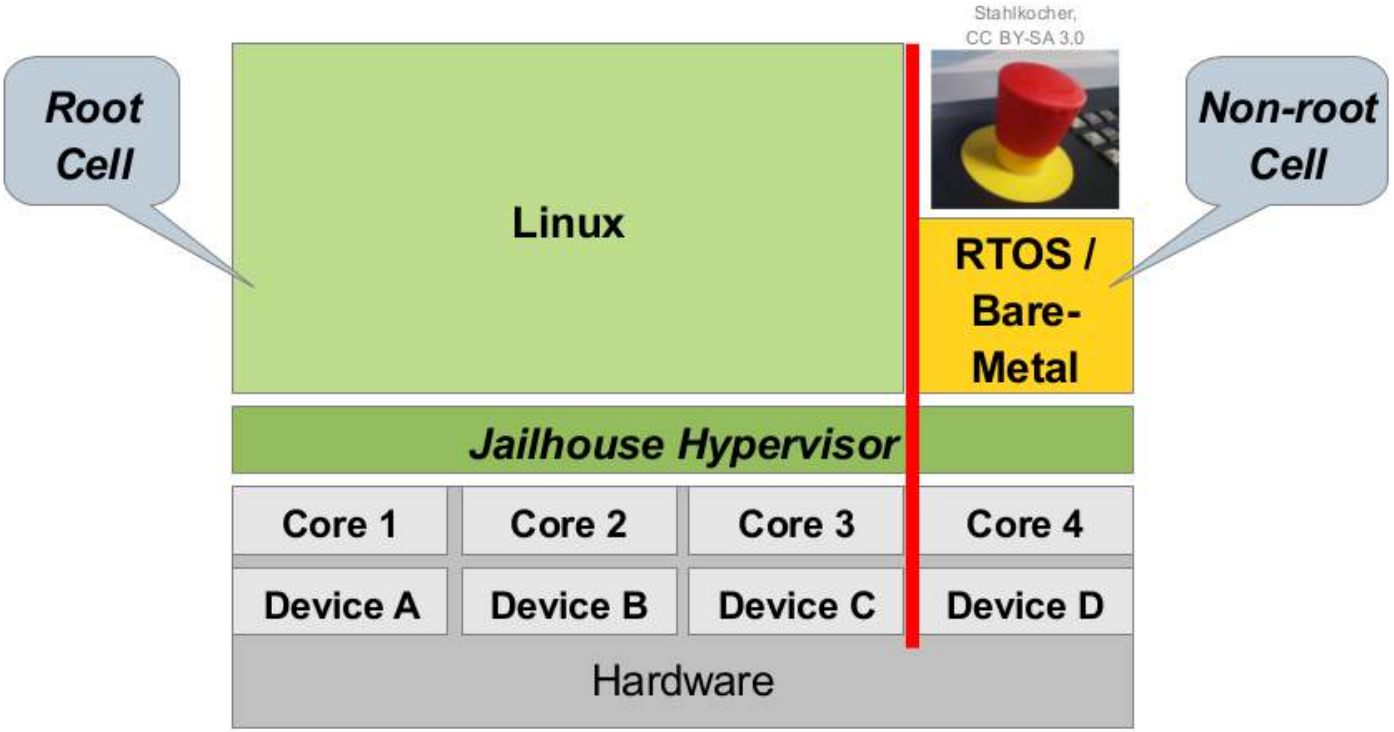


General requirements:

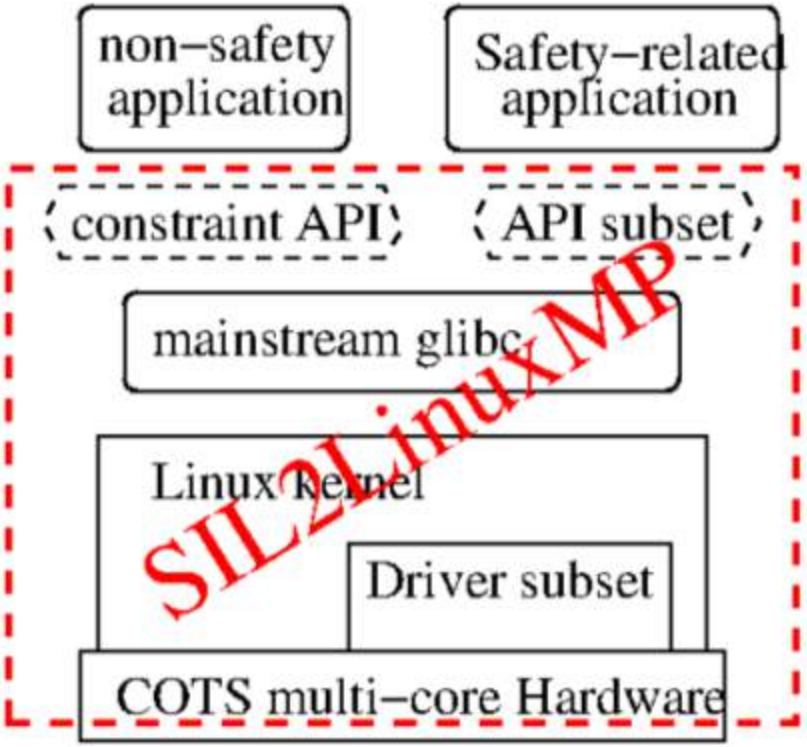
- **Linux** used on some components to fulfill **technical** and **commercial requirements**
- Functionality up to **safety integrity level (SIL) 2**

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

Гипервизор Siemens Jailhouse



OSADL SIL2LinuxMP



Linux или не Linux?

www.ghs.com/linux.html

Search

Green Hills SOFTWARE

Leading the Embedded World

INTEGRITY GLOBAL SECURITY

Linux in Defense

White Papers

Part I: FAA Safety-critical Certified Operating Systems Deliver The Reliability and Security Required by Defense Systems; Linux Does Not

Part II: "Many Eyes" - No Assurance Against Many Spies

Part III: Linux Security: Unfit for Retrofit

Part IV: Linux in Defense: Free Software is Just Too Expensive

Part V: Linux in Defense: An Urgent Threat to National Security

Articles

EE Times - Linux: unfit for national security? (pdf)

Federal Computer Week - The Outsourcing Hole (pdf)

COTS Journal - Linux for Embedded Systems? (pdf)

Benchmark results - Green Hills Optimizing Compilers Shrink Linux, Outperform GNU

Embedded News

26-May-2015
Green Hills Software to Present and Exhibit at TU Automotive Detroit 2015 in Novi, MI

13-May-2015
LDRA and Green Hills Software Deliver Industry-Leading Multicore Development and Verification

6-May-2015
Green Hills Software Announces Compiler 2015

28-Apr-2015
Green Hills Software to Present and Exhibit at the Embedded

Linux или не Linux?

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

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.

Partitioned Operating Kernel (POK)

- Аспирантский проект Julien Delange (ParisTech)
  - 2007-2009 год
  - http://pok.tuxfamily.org/
- Единственная свободная ARINC-653-совместимой ОСРВ
- Лицензия BSD
- Работает в Qemu-x86, LEON
- Размер:
  - Ядро — 8 тыс. строк
  - libpok — 16 тыс. строк

Наши доработки (1)

- Приведена в соответствие со стандартом (1)
- Удалена поддержка Ada
- Разработан драйвер для сетевого взаимодействия по virtio
- Генерация конфигурации из MASIW
- Поменяли лицензию на GPLv3
- Статистика
  - 107 коммитов
  - 194 files changed, 10814 insertions(+), 5642 deletions(-)
- Поддержка аппаратуры:
  - Qemu-x86

Наши доработки (2)

- Приведена в соответствие со стандартом
- Портирована на PowerPC
- Разработан драйвер консоли
- Переписана система сборки
- Статистика:
  - 280 коммитов
  - 879 files changed, 20857 insertions(+), 37426 deletions(-)
- Поддержка аппаратуры:
  - Qemu-x86
  - Qemu-PowerPC
  - Freescale QorIQ P3041

Свободная ОСРВ ИСП РАН

kernel:

Language	files	blank	comment	code
C	69->82(+13)	1453->2263(+810)	1706->2465(+759)	5508->8218(+2710)
C Header	58->84(+26)	616->1049(+433)	1208->3335(+2127)	1758->3182(+1424)
Assembly	5->5(0)	160->145 (-15)	159->183(+24)	765->750(-15)
SUM:	132->171(+39)	2229->3457(+1228)	3073->5983(+2910)	**8031->12150(+4119)**

177 files changed, 12526 insertions(+), 5800 deletions(-)

libpok:

Language	files	blank	comment	code
C	266->257(-9)	2657->2801(+144)	9042->9262(+220)	13034->13738(+704)
C Header	56->57(+1)	761->799(+38)	1782->1848(+66)	2894->3064(+170)
Ada	12->0	9->0	122->0	556->0
Assembly	2->2	0->0	0->0	24->24
SUM:	324->316(-8)	3418->3600(+182)	10824->11110(+286)	**15952->16826(+874)**

172 files changed, 3296 insertions(+), 3462 deletions(-)

Планы

- Поддержка POSIX партиций
- Частичная поддержка ARINC-653 часть 2
- Драйвера для QorIQ P3041 Ethernet
- Сетевой стек (IPv4+UDP+TFTP)
- gdb сервер для отладки ядра на железе
- Мега цель - сертификационный пакет
  - требования
  - дизайн проект
  - тесты

LinuxTesting.org

Спасибо!

Алексей Хорошилов
khoroshilov@ispras.ru
https://forge.ispras.ru/projects/chpok

ИСП РАН
Институт системного программирования РАН