Проектирование и разработка авионики: перспективы свободного программного обеспечения

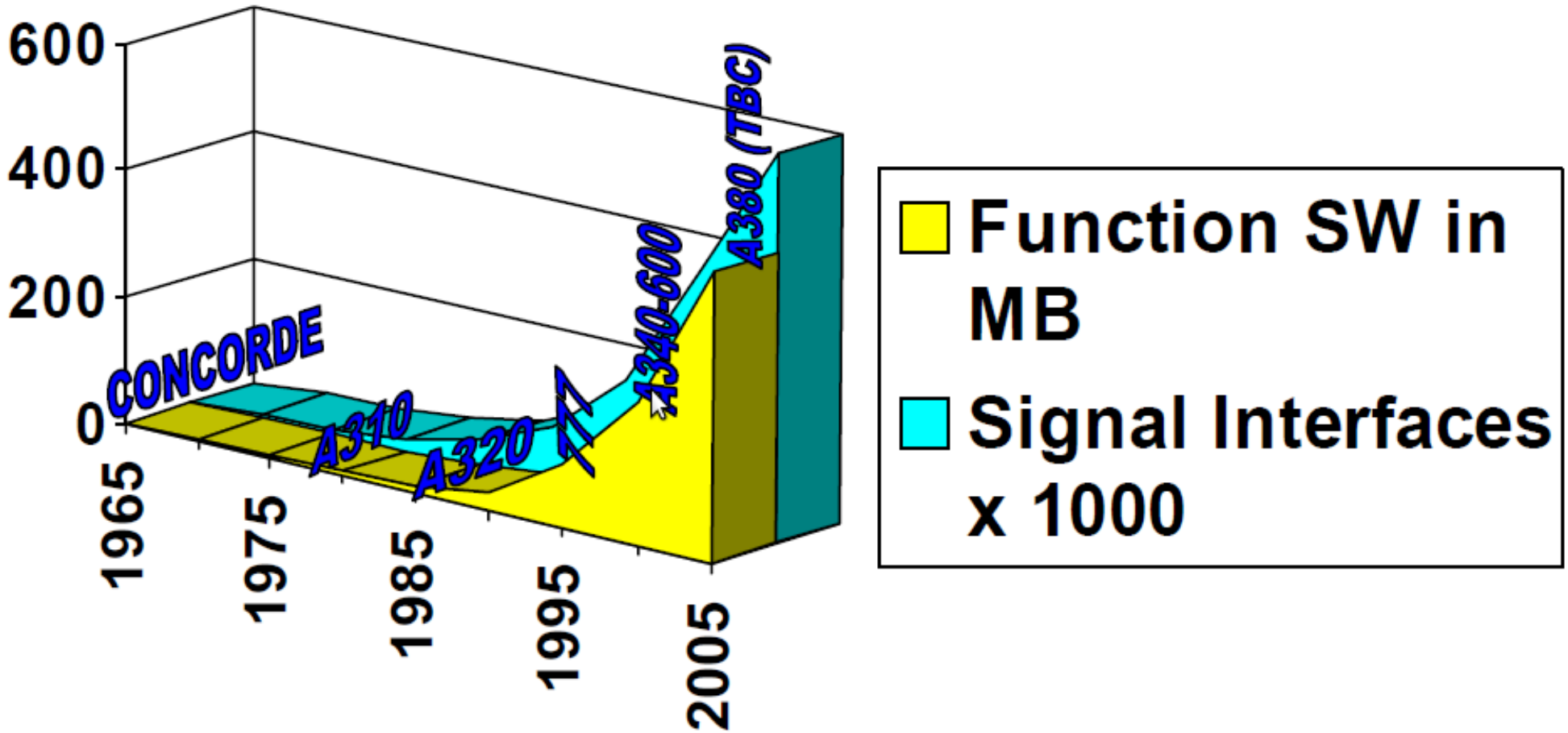
Хорошилов Алексей
khoroshilov@ispras.ru

ISP RAS

Ответственные системы (1)

Ответственные системы (2)

Рост применения авионики (1)



Рост применения авионики (2)

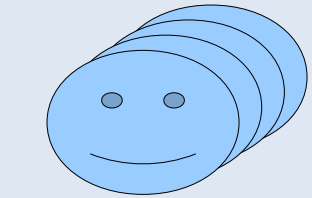
Обеспечение безопасности

- **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
- ...

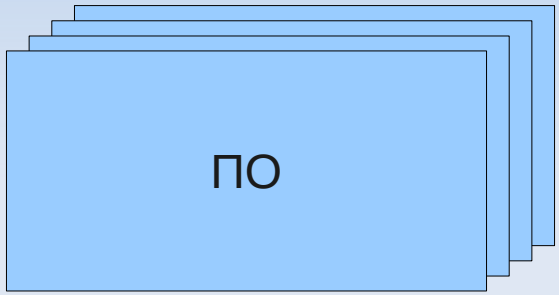
Категории отказных ситуаций

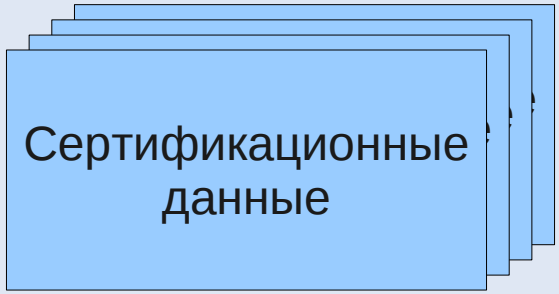
- Категория A – Катастрофическая
  - Препятствует безопасному функционированию объекта управления
- Категория B – Опасная / критическая
  - Приводит к критическому уменьшению возможностей объекта управления или способности персонала справиться с неблагоприятными режимами
- Категория C – Существенная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

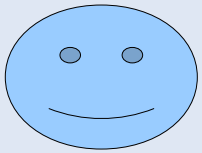
Сертификация ПО



разработчик



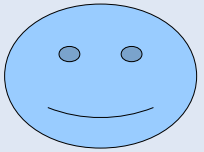




интегратор

бортовой комплекс

Комплект сертификационных документов



орган сертификации

Сертификационные данные

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

  до 18 видов документов

Мифы или реальность?

- СПО не применимо для использования в ответственном ПО, так как:
  - качество СПО не достаточно для ответственных применений
  - невозможно сертифицировать код, который изначально не разрабатывался для сертификации
  - заинтересованное сообщество слишком мало для эффективности модели СПО
  - бизнес модель СПО не выгодна для ответственного ПО
  - это откроет ключевые знания компании конкурентам
  - разработчикам не интересно работать над сертификационными данными просто ради удовольствия

Мотивации внедрения и разработки СПО

- Снижение стоимости и времени выхода на рынок за счет переиспользования готового ПО
- Снижение стоимости развития ПО за счет распределение затрат между многими заинтересованными лицами
- Построение успешного бизнеса
- Создание конкурентной среды
- Организация децентрализованного исследования новых подходов
- Just for fun

Среда разработки 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

Компилятор gcc

- Wind River
- Monta Vista
- LynuxWorks
- Freescale
- QNX
- Mentor Graphics
- Xilinx

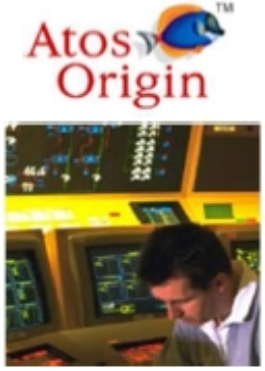
...

	gcc							
Низкое качество	–							
Невозможно сертифицировать	–							
Нет сообщества	N/A							
Нет бизнеса	N/A							
Ключевая ценность	N/A							
Не для хобби	N/A							
Переиспользование	+							
Распределение	N/A							
Бизнес	±							
Конкурентность	N/A							
Исследования	N/A							
Для хобби	N/A							

AdaCore GNAT

AdaCore
The GNAT Pro Company

A High Demanding Customer Base



	gcc	gnat						
Низкое качество	–	–						
Невозможно сертифицировать	–	–						
Нет сообщества	N/A	N/A						
Нет бизнеса	N/A	–						
Ключевая ценность	N/A	–*						
Не для хобби	N/A	N/A						
Переиспользование	+	+						
Распределение	N/A	+						
Бизнес	±	+						
Конкурентность	N/A	N/A						
Исследования	N/A	N/A						
Для хобби	N/A	N/A						

SIEMENS

Linux and safety-related systems

Some advantages of using Linux in embedded systems:

- **Cost reduction**: Many Linux distributions are royalty-free.
- **Reduced time to market**: Most of the commonly required features are available.
- **Protection of investment**: No vendor lock-in; standardized application programming interface.

→Linux has become the most popular embedded operating system.

Safety-related embedded systems:

- Software must be developed and used according to strict rules defined by safety standards.
- Safety standards deal very little with pre-existing software like Linux.

→Big uncertainty how to use Linux correctly in safety-related systems.

→Linux has not commonly been used in the area of safety-related systems up to now.

Linux and safety-related systems…
…at Siemens

SIEMENS

Software is an important part of most Siemens products, systems and services. In many cases the major part of the products' functionality is defined by software.

Software strategy at Siemens

- Product software providing ***differentiating*** features is protected via IPRs.
- For providing necessary but ***non-differentiating*** features, Open Source Software is an adequate instrument.

Product portfolio of Siemens

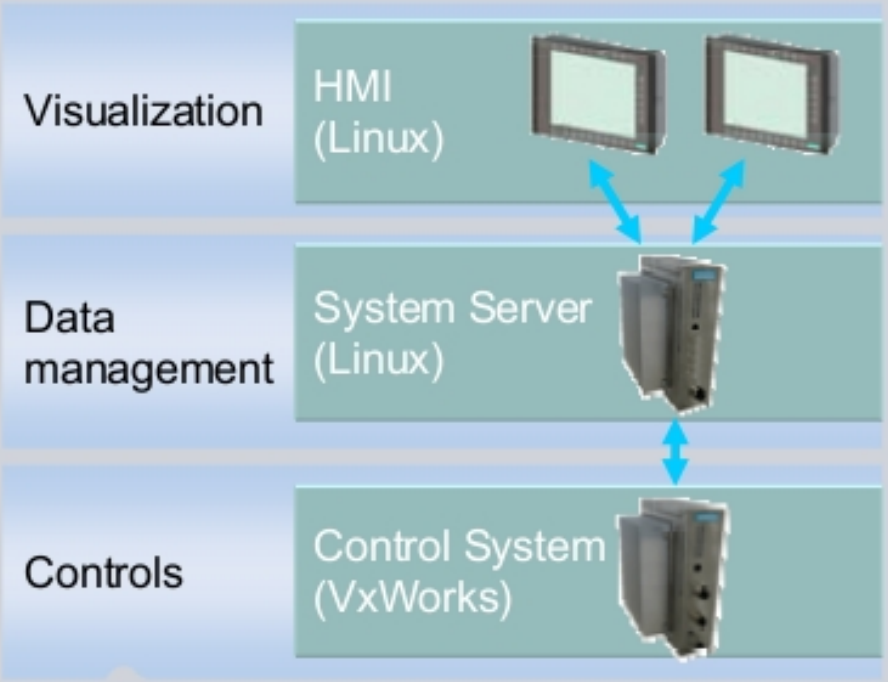
- Energy, Healthcare and Industry: Large share of the product software is for safety-relevant environments.

To benefit from the advantages of Linux in the big market of safety-related systems, a well-suited strategy and implementation is needed.

Project context: Linux-based vehicle control system

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?

Итоги

	gcc	gnat	Siemens					
Низкое качество	–	–	–					
Невозможно сертифицировать	–	–	–					
Нет сообщества	N/A	N/A	N/A					
Нет бизнеса	N/A	–	N/A					
Ключевая ценность	N/A	–*	N/A					
Не для хобби	N/A	N/A	N/A					
Переиспользование	+	+	+					
Распределение	N/A	+	+					
Бизнес	±	+	N/A					
Конкурентность	N/A	N/A	+					
Исследования	N/A	N/A	N/A					
Для хобби	N/A	N/A	N/A					

TOPCASED

Toolkit in Open-Source for Critical Application & Systems Development

First ideas

Partnership

Project kickOff

Aerospace Valley proposition

First steering committee

1st open source delivery

National funding

2004

2005

2006

Model editors (UML,SysML,...) + change management (gPM) + collaborative work

v 1.0

Start of experimentations

Improvements + first documentation generator + Verification (simulation and rules checkers)

v 2.0

Users feedback

Full model process + Model requirement traceability

v 3.0

2007

2008

Start of Industrial Improvements for A350 Deployment

2009

OPEES

TOPCASED

Toolkit in Open-Source for Critical Application & Systems Development

Original Goals

- To reduce development costs for embedded systems (Aeronautical, space and automative domains) by promote optimised process and tools : maturity, competitivity and time to market end product. Supports Model Based System Engineering.
- To insure durability of the toolkit through an Open source approach : limited market, very, very long life, editors durability, editors strategy, deployment facilities.
- To integrate current academic research results in industrial development process.
- To enforce Academics / Industries relationship
- To provide student engineers with knowledge of industrial process and related tools
- To enforce SMEs / Industries relationship

TOPCASED

Toolkit in Open-Source for Critical Application & Systems Development

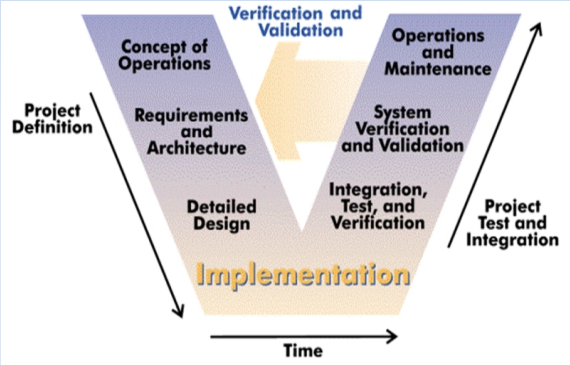
- 1M Line of Code
- Education of Engineer at University/School : more than 500
- Industrial projects : you will see today
- 50 developers
- 11 thesis as we known
- Strong relationship with Eclipse fondation
- A lot of research project
- Strong relationship between Academics/Industrial/SMEs
- Download around 6000/month

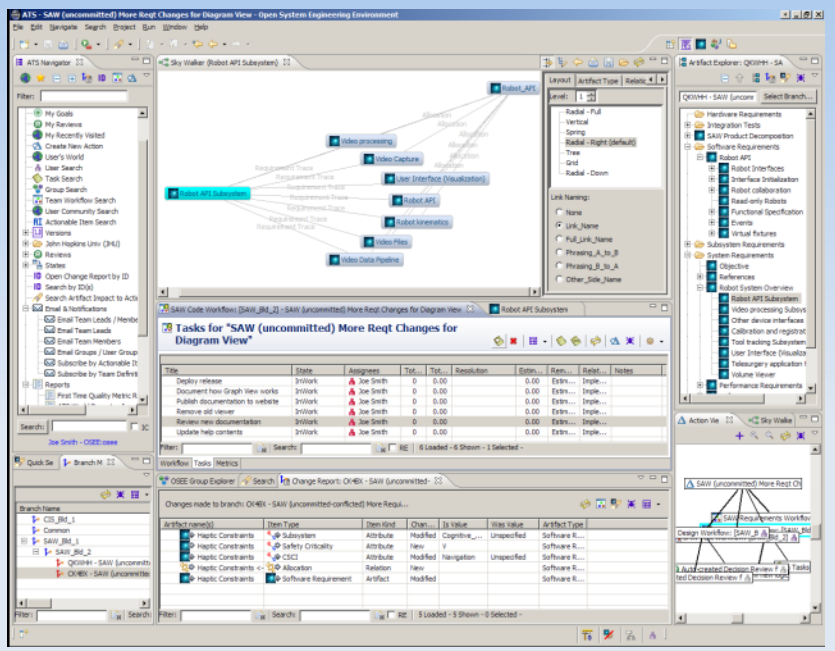
Итоги

	gcc	gnat	Siemens	TOP CASED				
Низкое качество	–	–	–	N/A				
Невозможно сертифицировать	–	–	–	N/A				
Нет сообщества	N/A	N/A	N/A	–				
Нет бизнеса	N/A	–	N/A	N/A				
Ключевая ценность	N/A	–*	N/A	N/A				
Не для хобби	N/A	N/A	N/A	N/A				
Переиспользование	+	+	+	N/A				
Распределение	N/A	+	+	+				
Бизнес	±	+	N/A	N/A				
Конкурентность	N/A	N/A	+	+				
Исследования	N/A	N/A	N/A	+				
Для хобби	N/A	N/A	N/A	N/A				

Boeing OSEE

Open System Engineering Environment is an integrated, extensible tool environment for large engineering projects





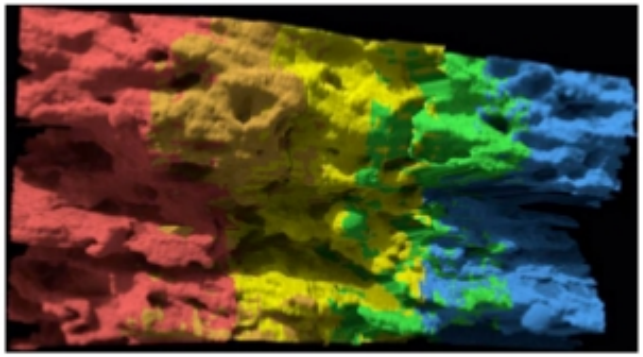
- Разработан Boeing для поддержки разработки системы управления полетом Apache Attack Helicopter
- Разрабатывается с 2004 года
- С 2007 года опубликован под Eclipse Public License как проект Eclipse Foundation

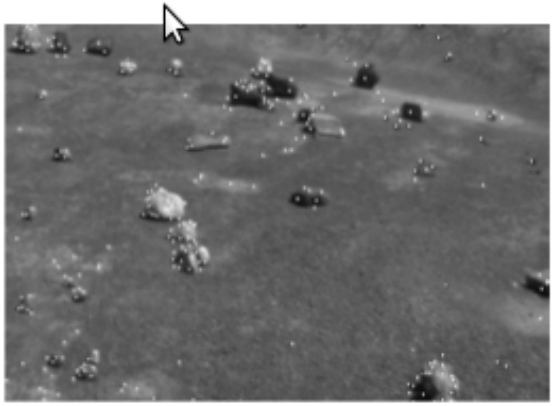
	gcc	gnat	Siemens	TOP CASED	OSEE			
Низкое качество	–	–	–	N/A	N/A			
Невозможно сертифицировать	–	–	–	N/A	N/A			
Нет сообщества	N/A	N/A	N/A	–	–			
Нет бизнеса	N/A	–	N/A	N/A	N/A			
Ключевая ценность	N/A	–*	N/A	N/A	N/A			
Не для хобби	N/A	N/A	N/A	N/A	N/A			
Переиспользование	+	+	+	N/A	N/A			
Распределение	N/A	+	+	+	+			
Бизнес	±	+	N/A	N/A	N/A			
Конкурентность	N/A	N/A	+	+	+			
Исследования	N/A	N/A	N/A	+	N/A			
Для хобби	N/A	N/A	N/A	N/A	N/A			

Vision Workbench (2006)

Overview

- Modular, extensible, C++ computer vision framework
- Rapid development and flexible, multi-platform (Linux, OS-X, Win32)
- Supports science analysis, robot perception, image stitching, etc.





Vision Workbench (2006)

Developers

- **Government**: NASA Ames Intelligent Systems Division
- **Prime Contractor**: QSS Group, Inc.
- **University**: Carnegie Mellon / Silicon Valley
- **Non-Profit**: Research Institute for Advanced Computer Science

Key points

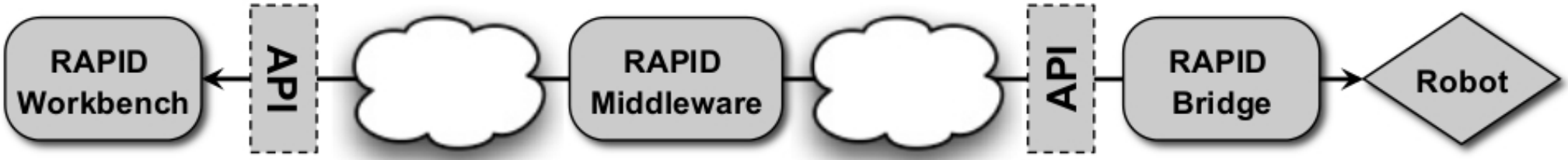
- Software library
  (continuous release / hosted on **GitHub**)
- Rapid, on-going development
- Supports numerous collaborations (funded & informal), interns, etc.
- Requires several external, open source libraries
  (OS licenses: Boost, MIT, BSD-like)
- Enhanced functionality with additional open source libraries
  (OS licenses: zlib/png, SGI, GPL2, etc.)

	gcc	gnat	Siemens	TOP CASED	OSEE	NASA Vision		
Низкое качество	–	–	–	N/A	N/A	N/A		
Невозможно сертифицировать	–	–	–	N/A	N/A	N/A		
Нет сообщества	N/A	N/A	N/A	–	–	–		
Нет бизнеса	N/A	–	N/A	N/A	N/A	N/A		
Ключевая ценность	N/A	–*	N/A	N/A	N/A	N/A		
Не для хобби	N/A	N/A	N/A	N/A	N/A	N/A		
Переиспользование	+	+	+	N/A	N/A	N/A		
Распределение	N/A	+	+	+	+	N/A		
Бизнес	±	+	N/A	N/A	N/A	N/A		
Конкурентность	N/A	N/A	+	+	+	N/A		
Исследования	N/A	N/A	N/A	+	N/A	+		
Для хобби	N/A	N/A	N/A	N/A	N/A	N/A		

RAPID (2009)

Overview

- "Robot Application Programming Interface Delegate"
- Standardized programming interface (API) for robot software
- Messaging & data distribution for NASA robots & user interfaces



RAPID (2009)

Developers

- **Government**: NASA Ames (Code TI) & Johnson (Code ER)
- **Prime Contractor**: SGT, Inc.
- **Subcontractor**: TRACLabs, Inc.
- **Non-Profit**: Research Institute for Advanced Computer Science

Key points

- Software suite: libraries, user interface, reference implementation (hosted on **SourceForge**)
- Facilitates basic research & collaboration worldwide (does not require SUA / other agreement that would be extremely difficult to execute)
- De-facto NASA robotics open standard

Итоги

	gcc	gnat	Siemens	TOP CASED	OSEE	NASA Vision	NASA Rapid	
Низкое качество	–	–	–	N/A	N/A	N/A	–	
Невозможно сертифицировать	–	–	–	N/A	N/A	N/A	N/A	
Нет сообщества	N/A	N/A	N/A	–	–	–	–	
Нет бизнеса	N/A	–	N/A	N/A	N/A	N/A	N/A	
Ключевая ценность	N/A	–*	N/A	N/A	N/A	N/A	N/A	
Не для хобби	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
Переиспользование	+	+	+	N/A	N/A	N/A	+	
Распределение	N/A	+	+	+	+	N/A	+	
Бизнес	±	+	N/A	N/A	N/A	N/A	N/A	
Конкурентность	N/A	N/A	+	+	+	N/A	N/A	
Исследования	N/A	N/A	N/A	+	N/A	+	+	
Для хобби	N/A	N/A	N/A	N/A	N/A	N/A	N/A	

Garbee Rockets

Итоги

	gcc	gnat	Siemens	TOP CASED	OSEE	NASA Vision	NASA Rapid	Garbee Rockets
Низкое качество	–	–	–	N/A	N/A	N/A	–	N/A
Невозможно сертифицировать	–	–	–	N/A	N/A	N/A	N/A	N/A
Нет сообщества	N/A	N/A	N/A	–	–	–	–	N/A
Нет бизнеса	N/A	–	N/A	N/A	N/A	N/A	N/A	N/A
Ключевая ценность	N/A	–*	N/A	N/A	N/A	N/A	N/A	N/A
Не для хобби	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Переиспользование	+	+	+	N/A	N/A	N/A	+	+
Распределение	N/A	+	+	+	+	N/A	+	N/A
Бизнес	±	+	N/A	N/A	N/A	N/A	N/A	N/A
Конкурентность	N/A	N/A	+	+	+	N/A	N/A	N/A
Исследования	N/A	N/A	N/A	+	N/A	+	+	N/A
Для хобби	N/A	N/A	N/A	N/A	N/A	N/A	N/A	+

Выводы

- СПО пригодно для ответственных систем
- СПО как инструмент для организации исследований и переиспользования СПО общего назначения
- Сертификационные данные как дополнительная возможность для бизнеса
- Подготовка сертификационных данных как хобби не распространено

Спасибо за внимание!

Хорошилов Алексей
khoroshilov@ispras.ru

ISP RAS