Интеллектуальная управляемость ПО и вопрос доверия

Дагаев Дмитрий Викторович,
Главный Эксперт,
АО «Русатом Автоматизированные системы управления»,
Проект «Информатика-21», dvdagaev@mail.ru

Ермаков Илья Евгеньевич,
Системный проектный центр Ermakov Systima, ie@iermakov.ru

Ткачёв Фёдор Васильевич,
д. ф.-м. н., вед. н. с. ИЯИ РАН,
Координатор проекта «Информатика-21», info21@inr.ac.ru

Об интеллектуальной управляемости

«Было открыто несколько правил, нарушение которых либо существенно ослабляет, либо вовсе разрушает ***интеллектуальную управляемость программы***. Эти правила делятся на два вида.

Правила первого вида накладываются автоматически выбором адекватного ***языка программирования***.

Правила второго вида представляют собой элементы ***дисциплины, требуемой от программиста***.»

Э.Дейкстра «Смиренный программист», тьюринговская лекция.

Стратегическое видение Дейкстры , Тьюринговская лекция, 1972

О прошлом

Язык программирования ***ускользает из-под контроля нашего интеллекта***.

Главный источник его проблем (PL/1) кроется в том, что в нем уже и так слишком уж много "возможностей“.

Разработка "более богатых возможностями" или "более мощных" языков программирования была ошибкой ... неуправляемы ментально.

О будущем

Придерживаться разработки только интеллектуально-управляемых программ.

Предоставить убедительное доказательство корректности программ.

Великое ***будущее для очень систематических и очень умеренных языков***.

Свойственные человеку ограничения позволяют решать только хорошо структурированные задачи.

Выбор Хоара, Тьюринговская лекция, 1980

«Другой — сделать ПО таким сложным, чтобы не было ***очевидных*** недостатков.» Э.Хоар

Старые платья императора нарастают одно на другое в виде культурных слоев, обратного хода нет.

Система в один прекрасный день рушится, и императора под ней уже нет.

«Один способ — сделать ПО таким простым, чтобы было ***очевидно***, что недостатков нет»

Великая сила Паскаля, что в нем очень мало ненужных свойств и почти нет нужды в подмножествах. Вот почему этот язык достаточно силен, чтобы выдержать специализированные расширения

Аргументация Вирта для Проекта Оберон

Неконтролируемый рост ПО ограничивается только возможностями железа.

Обилие функциональности как критерий мощности ПО с точки зрения бизнеса.

Некачественный монолитный дизайн с навязываем потребителю всех возможностей.

“Мольба о простоте ПО (A plea for the lean SW)”.

1. ***Простота***, ограничение лишь существенными особенностями системы.
2. Объектно-ориентированный язык, обеспечивающий безопасность типов.
3. Модульность и расширяемость типов. Динамическая наращиваемость.

Тест на интеллектуальную воспроизводимость ПО

Проект Оберон (ОС, компилятор, графика) содержит < 20 тыс строк, 120 Кбайт.

Вопрос Гуткнехту: Можно ли воссоздать ***Проект Оберон*** по памяти на необитаемом острове без интернета?

Ответ: Да, была бы отличная дипломная практика.

Человеческий интеллект ***ограничен***, но в нем уместится информационный объем Проекта Оберон.

Риторический вопрос: А ***GCC***?

Вопрос доверия

«Хочешь накормить человека один раз — дай ему рыбу. Хочешь накормить его на всю жизнь — научи его рыбачить»

Конфуций

«Целью обеспечения доверия является создание уверенности в надёжном функционировании продукта в заданных условиях.»

ГОСТ Р 54583-2011/ISO/IEC/TR 154443-3:2007

Вопрос, видимо, в людях и в интеллектуальной управляемости.

Есть такая партия!
Географический пояс Оберона

Активные разработчики образуют на карте пояс Оберона. Географический пояс Оберона сильно гармонирует с государственной стратегией Китая «Один пояс один путь».

К обсуждению практических возможностей повышения защищенности, устойчивости систем.

Мульти компилятор — многоцелевая система

МультиОберон 0.9 https://github.com/dvdagaev/Mob это интеграционный проект компилятора языка Оберон с различными сменными бэкендами (прорабатываемые отмечены *).

	Наименование	Реализация
Omb32 - BlackBox	Генерация нативного кода x86 для системы BlackBox	POSIX X86
Omf32/64 - Ofront	Транслятором Ofront в язык C	Везде
Oml32/64 - Ofront	Генератором биткода LLVM	Aarch64, AMDGPU, ARM, BPF, Hexagon, Lanai, MSP430, Mips, NVPTX, PowerPC, Sparc, SystemZ, X86, XCore
Oma2 – A2 *	Кодогенерация для системы A2	OS A2
Omemb – Embedded bare metal *	Кодогенерация в нативный код встроенных систем	Без OS, компактный runtime
Omace *	Рассматривается возможность гибридного программирования	Прототип – Active Cells

МЭК 60880 – обеспечение функциональной безопасности систем для АЭС категории А

B.2cb Избегать использования универсальных ОС ~~**std OS**~~;

B.2cd OS должна содержать только необходимые функции ~~**stdlib**~~;

B.4ag Циклы только с постоянными максимальными областями значений переменной цикла ~~**WHILE REPEAT LOOP**~~;

B.2dd Время прогона не должно существенно меняться от изменения входных данных ~~**IF**~~;

B.2ee Применение или блокирование прерываний должно быть тщательно оформлено документально ~~**INTR**~~;

B.4dc Массивы должны иметь фиксированную длину ~~**NEW**~~;

Обеспечение соответствия требованиям ФБ определяется ***отсутствием***, а не наличием функциональности.

RESTRICT – Ограничения использования

RESTRICT дает профилактическую защиту ПО против «хирургии последствий».

Операция RESTRICT ‘–’ отключает операторы, ‘+’ восстанавливает отключенные, а ‘*’ ограничивает их использование заранее определенным образом.

Для адаптирования к стандарту 60880 потребуется нижестоящее определение и вариант бэкенда, который это поддерживает. Отключаем ~~NEW, WHILE, LOOP, REPEAT, CASE/ELSE~~. Отключаем ~~рекурсию~~.

```
RESTRICT –NEW –WHILE –LOOP –REPEAT –ELSE(CASE)
  +EXIT(FOR)-”Recursion”;
```

Близкая аналогия – Ada Restrictions.

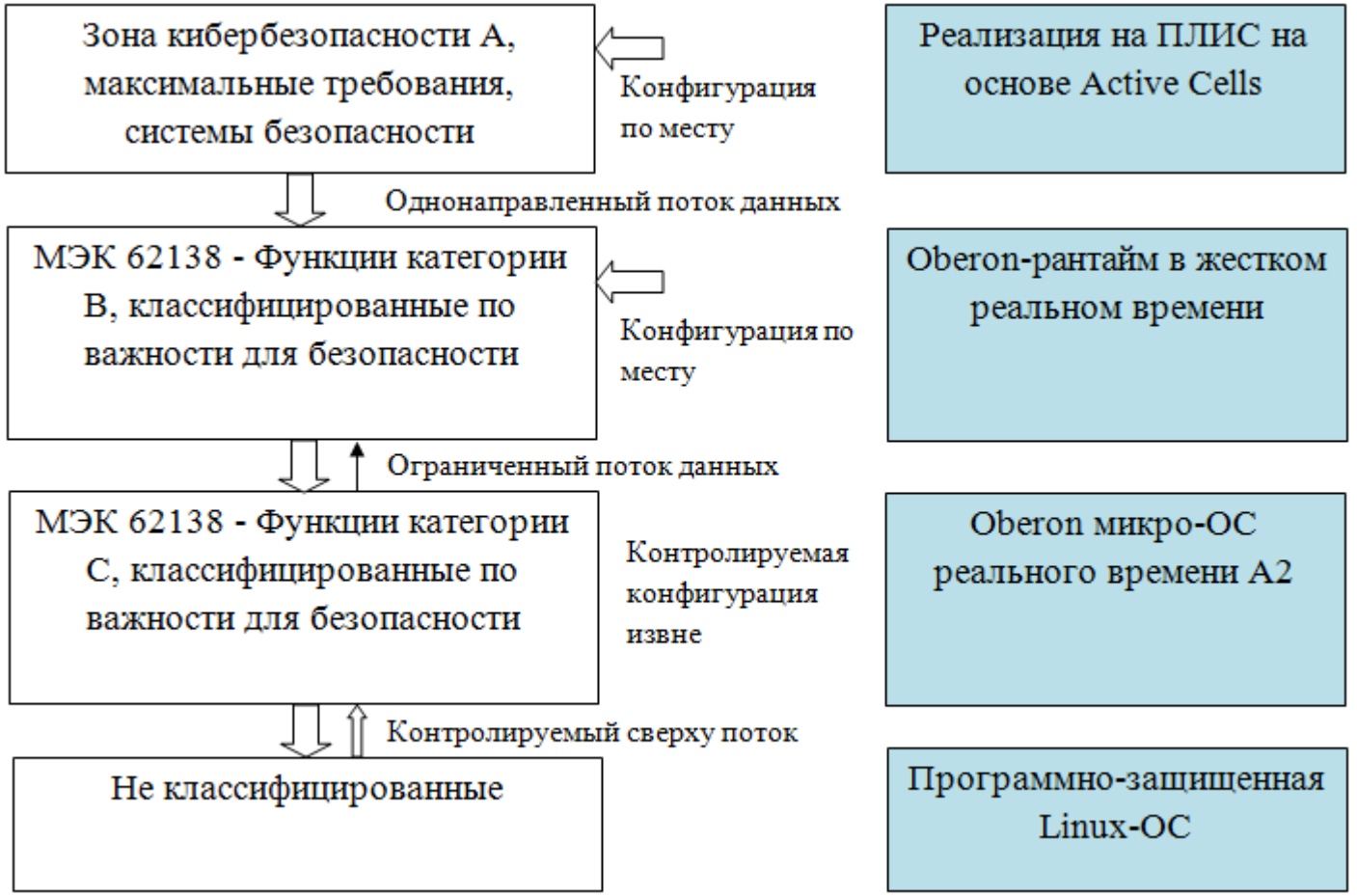
```
pragma Restrictions (No_Recursion);
```

Варианты реализации систем и интеллектуальная управляемость

- Программно-защищенная Linux-ОС ??% (серая зона), компилятор 90%, прикладное ПО 100%;
- Аппаратно-защищенная Oberon микро-ОС A2 90%, компилятор 90%, прикладное ПО 100%;
- Аппаратно-защищенный Oberon-рантайм в жестком цикле реального времени 100%, прикладное ПО 100%;
- Аппаратная защищенная реализация на ПЛИС прикладного ПО 100% (на основе технологии Active Cells).

МЭК 62645 – Требования по защищенности программ СКУ

Разбиение на зоны безопасности и переход к рассмотрению распределенных систем



Базовый уровень: Безопасность языка Оберон и явные схемы

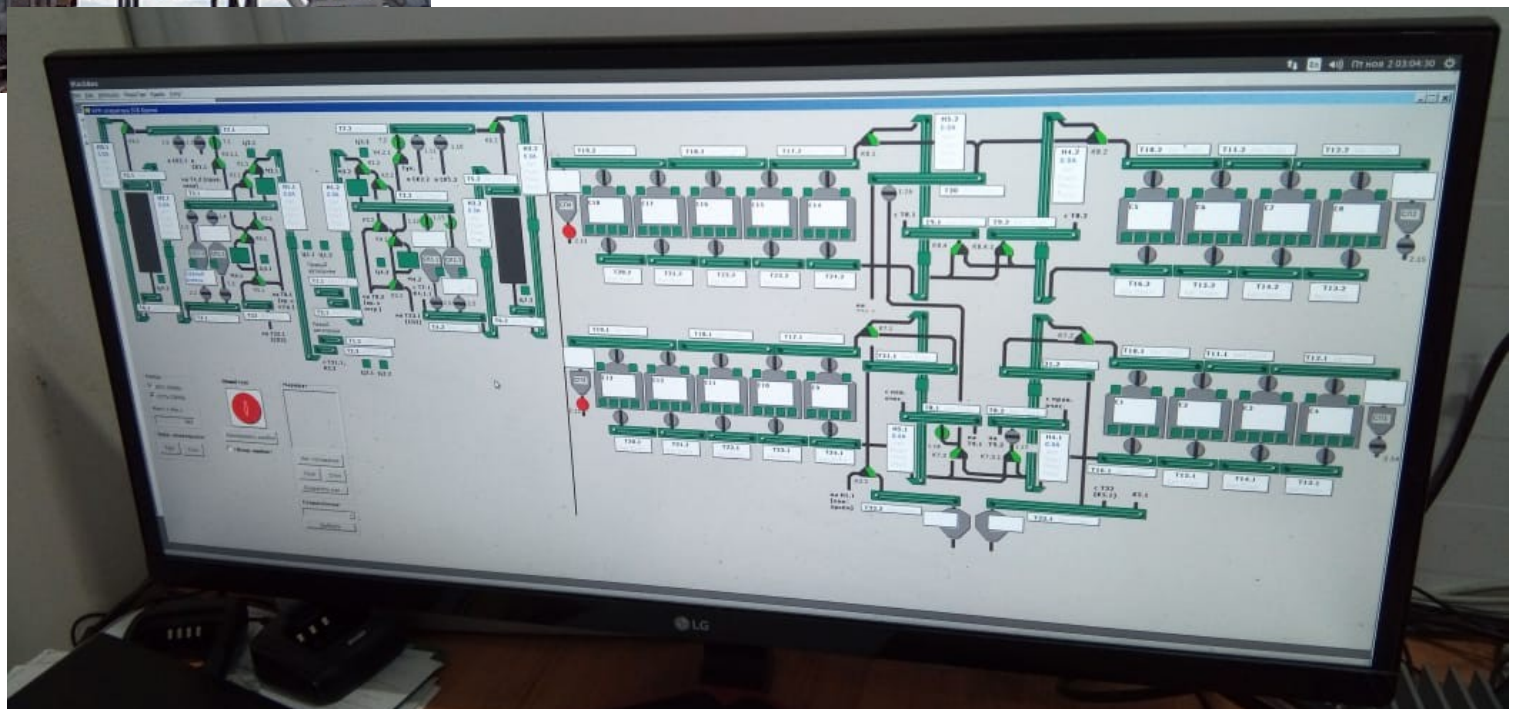
- Безопасность типов, статическая типизация;
- Безопасность и контроль границ массивов;
- Безопасность указателей, автоматическое управление памятью;
- Безопасность наследования, отсутствие неявных схем наследования реализации, хрупкие базовые классы;
- Безопасность взаимодействия в виде реализации мониторов Хансена-Хоара в активных объектах A2;
- Безопасность работы с динамически загружаемыми модулями с контролем зависимостей интерфейсов;
- Безопасность используемых библиотечных процедур.

Оберон (Блэкбокс) в АСУТП

SCADA-платформа

ERSY Control

- на базе BlackBox Component Builder



Автоматизация крупных объектов АПК

(холдинг МираТорг)

Оберон (Блэкбокс) в АСУТП

Siemens WinCC, TIA Portal:

10-20 Гб инструментарий и конечные сборки

Операторские интерфейсы:

браузер (10-20 млн. строк кода), Flash, Silverlight, …

Owen 4D с Master SCADA:

- Внутри ПЛК: ОС Linux, интерпретатор Lua (со сборкой мусора), интерпретатор МЭК-языков, веб-сервер…

SCADA на базе BlackBox:

- 20-40 Мб инструментарий и конечные сборки;
- Своя кроссплатформенная графическая система, поддержка документов и иерархических компонентных интерфейсов, без толстых «бытовых» прослоек (браузеров, Flash и т. п.).

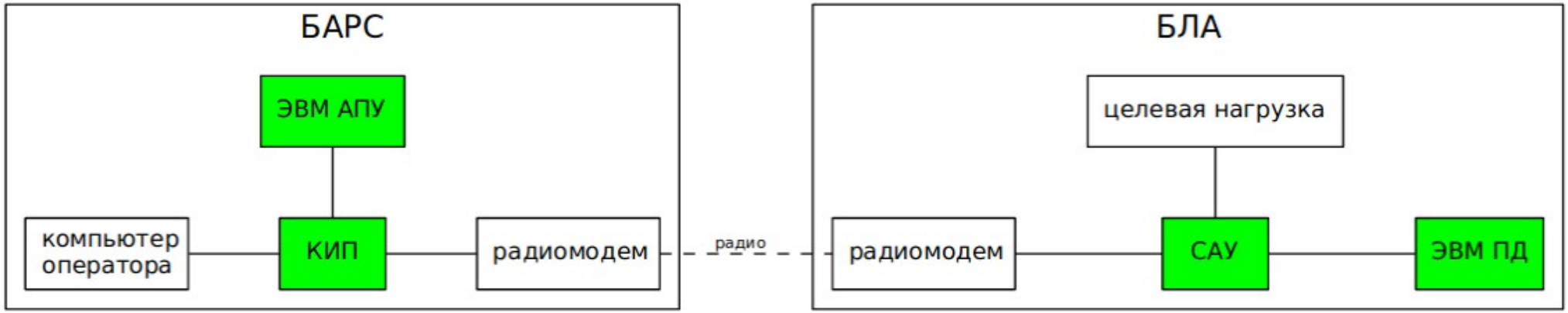
На голом железе

Экотрас, Ширяев А.В.

- Компилятор O7 Александра Ширяева: Oberon-07 для ARM

Комплекс БЛА:

Бортовое и наземное ПО, на базе STM, без ОС



Информатика-21

Международный общественный научно-образовательный проект

http://www.inr.ac.ru/~info21/

Единая система **базовых курсов информатики** от 5 класса до 3-4 курса университетов, на основе Компонентного Паскаля и системы Блэкбокс **как единой платформы**

Как оказалось, требования в образовании и в критических отраслях – одинаково жёсткие.

Показанные выше применения Оберона в России

(АЭС, БЛА, физика высоких энергий, АСУТП)

сложились вокруг опыта проекта Информатика-21.

Ежегодная отраслевая конференция «Оберон-технологии, образование и проблема качества в цифровой индустрии»

https://oberoncore.ru/oberonconf (доступны видео докладов)

Объединила ряд отраслевых и научных экспертов — на основе общих профессиональных ценностей и взглядов на развитие цифровой индустрии в направлении роста качества и ответственности решений.

Почётный член Программного комитета – проф. Юрг Гуткнехт.

Вопросы по докладу …

Дагаев Дмитрий Викторович,
Главный Эксперт,
АО «Русатом Автоматизированные системы управления»,
Проект «Информатика-21», dvdagaev@mail.ru

Ермаков Илья Евгеньевич,
Системный проектный центр Ermakov Systima,
ie@iermakov.ru

Ткачёв Фёдор Васильевич,
д. ф.-м. н., вед. н. с. ИЯИ РАН,
Координатор проекта «Информатика-21», info21@inr.ac.ru