Технологический стек Оберон-решений для разработки систем управления

Дагаев Дмитрий Викторович,

Главный Эксперт,

АО «РАСУ»,

Ермаков Илья Евгеньевич,

Управляющий партнёр,

Ermakov Systima

30 лет языку Оберон

- Н. Вирт, Университет ETHZ: Pascal – Modula-2 – Oberon (1988)
- Modula-2 и Oberon – вместе с ПК и ОС
- «Project Oberon» – полный стек:
- RISC CPU на ПЛИС (с 2013 года)
- Компилятор, ОС, оконная система, документно-объектная модель, редакторы (вёрстка и графика) – вмещаются в одну книгу «Project Oberon» вместе с исходными текстами (в т.ч. ЦПУ на ПЛИС)
- Стек для образования и критические применения (требования, оказывается, похожи)

30 лет языку Оберон

- Университет ETHZ и Оберон-школа: выпускники и совместные проекты, влияние на Sun, MS Research, Mozilla и т. д.
- Оберон – языковое ядро современного мейнстрима на 16 страницах: императив, ООП (расширение типов), строгая типизация, контроль границ массивов, герметичная работа с указателями, сборка мусора (отключаемая)

30 лет языку Оберон

- Модель Оберона победила в Java, C# и, наконец, в Google Go (самый компактный потомок Оберона, см. лекцию Роберта Гризмера «Эволюция языка программирования Go»)
- Только Оберон – на том же расстоянии от машины, что и Си, при этом убирая проблемы строгой типизацией (выход за границы массивов – > 90% уязвимостей софта) и компактно вводя ООП, модульность и компонентность (динамическая загрузка-выгрузка модулей, рефлексия и метапрограммирование)

Промышленные версии Оберона

- Современная Оберон-ОС A2 и её применения во встроенных системах, мультимедиа и др.
- Oberon-07 – современный диалект языка от Никлауса Вирта, множество реализаций под разные платформы, набирает популярность как надёжная замена Си для микроконтроллеров

Промышленные версии Оберона

- **Component Pascal и среда BlackBox** (Oberon Miscrosystems AG) – ныне open-source, BSD-подобная лицензия
- Применения в мире: АСУТП ГЭС, моделирование истребителя Eurofighter, DuPont, Mobatec Modeller… Штучные, ответственные проекты.
- Язык + компонентная среда IDEE (development & EXECUTION environment), фреймворк составных документов для научной и инженерной графики
- < 40 Мб, ~ 120 тыс. строк исходного кода – несколько групп компетенции в мире и России, способных на полную поддержку и развитие
- MS Windows, GNU/Linux, FreeBSD

Component Pascal / BlackBox

- Система выполнения ~ 3 тыс. строк кода.
- В ней: GC, метаинформация/рефлексия, динамическая загрузка/выгрузка модулей, обработка исключений.
- Архитектор КП/ББ – Клеменс Шиперски, далее – соархитектор платформы .NET

Оберон в России

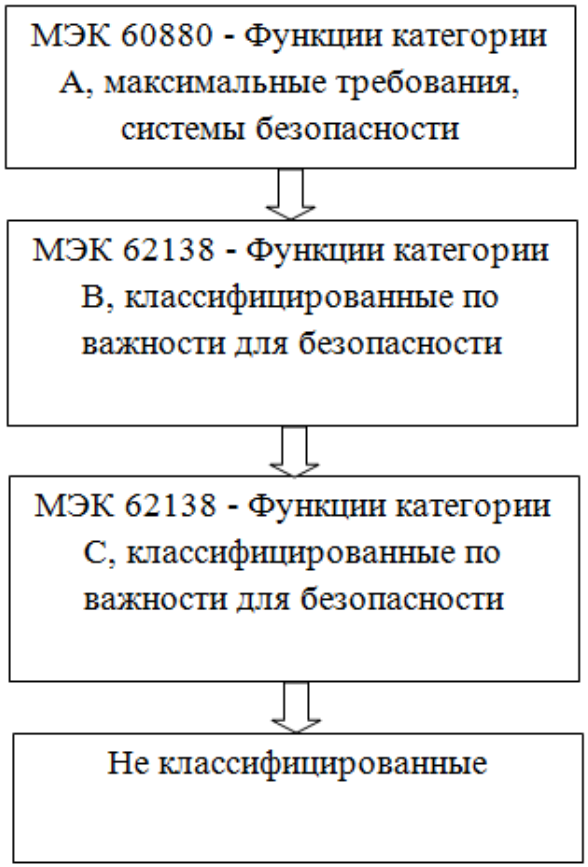
- Новосибирская школа – с 80-х годов. Компиляторы, ОС Excelsior – на ПК «Кронос» (часть проекта МАРС, ВНТК «СТАРТ»)
- Ныне компания Excelsior. XDS Oberon-2/Modula-2 – основа для стека бортового ПО в ИСС им. академика Решетнева (спутники связи и ГЛОНАСС, науч. рук. – А. А. Колташёв, научная школа Ершова/Поттосина)
- Excelsior JET – компилирующая реализация Java (часть реализации – на Oberon-2)

Оберон в России

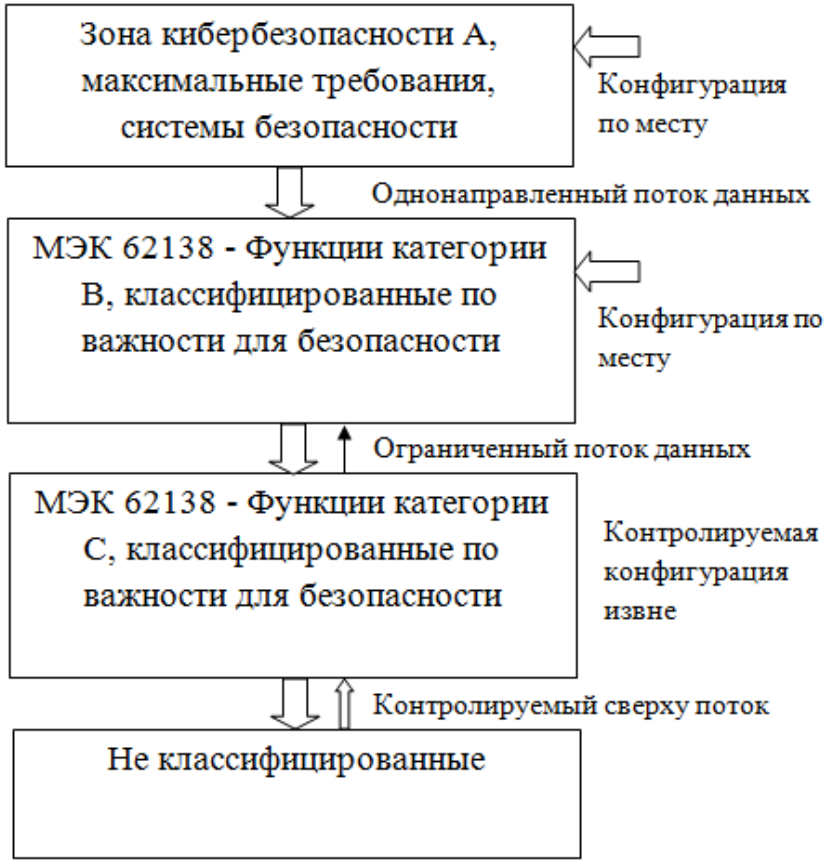
- Оберон-сообщество и проекты развиваются вокруг проектов «Информатика-21» (с 2002 г.) и OberonCore (с 2005 г.)
- На сегодняшний день проекты: уникальное ПО физики высоких энергий (символьная алгебра и др.), бортовое управляющее ПО (БПЛА), САРП АЭС, АСУТП в энергетике и агропроме, научное и встроенное ПО в биофизике, веб-сервисы.
- **См. материалы конференции «Оберон-технологии, образование и проблема качества в цифровой индустрии» (2018):**
- https://oberoncore.ru/oberonconf

Классификация подсистем для АЭС по уровню требований

МЭК 61513 - Функциональная безопасность АЭС



МЭК 62645 - Защищенность от кибер-угроз АЭС



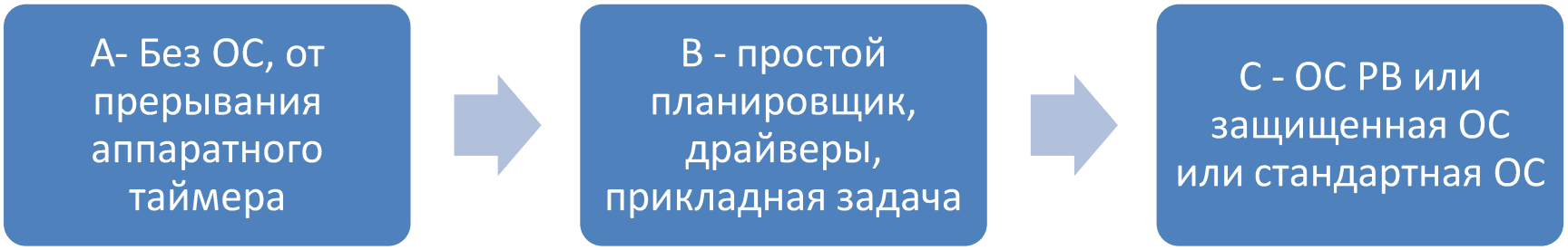
Необходимость технологического стека систем управления

- Категория А:
  - Без ОС (микро ОС) или ПЛИС, РВ с гарантированным аппаратным циклом, ограничение прерываний, циклическая передача данных, специализированные языки и компиляторы;
- Категория В:
  - Предпочтение микро ОС в части обеспечения РВ, надежности и сертификации, сертификация компиляторов, надежные решения для SCADA и контроллеров;
- Категория С:
  - Сертификация разработанных и используемых программных продуктов, надежные решения для SCADA и контроллеров;
- Неклассифицированные:
  - Полнофункциональные серверные и клиентские решения для построения на их основе высокоуровневых систем обработки, содержащие сложные математические расчеты.

Релевантные проекты Оберон-сообщества (только в РФ)

- Категория А:
  - Управляющее ПО для беспилотных летательных аппаратов + разработанный компилятор (А.В.Ширяев);
- Категория В:
  - Система аварийной регистрации параметров (САРП) 1 энергоблока Ростовской АЭС - (Д.В.Дагаев);
- Категория С:
  - АСУТП в агропроме («МираТорг») (И.Е.Ермаков);
- Неклассифицированные:
  - Программа для обработки данных научной установки ИЯИ РАН «Троицк ню-масс» (Ф.В.Ткачев).
  - Программа для класса задач компьютерной алгебры в физике , устранение 10-летнего рассогласования теории и эксперимента в распадах b-кварка (Ф.В.Ткачев).

Стек масштабируемых решений



Оберон-сообщество движется в сторону создания интегрированных решений, каждое из которых может быть реализовано в разных средах исполнения. Используются компиляторы со сменными бэкендами для генерации кода для разных платформ.

Вся линейка решений позволит наилучшим способом выбрать подходящие средства для реализации систем управления с сохранением во всех вариантах присущих Оберонам гарантий строгости на уровне компилятора.

Стратегия переносимости и адаптации

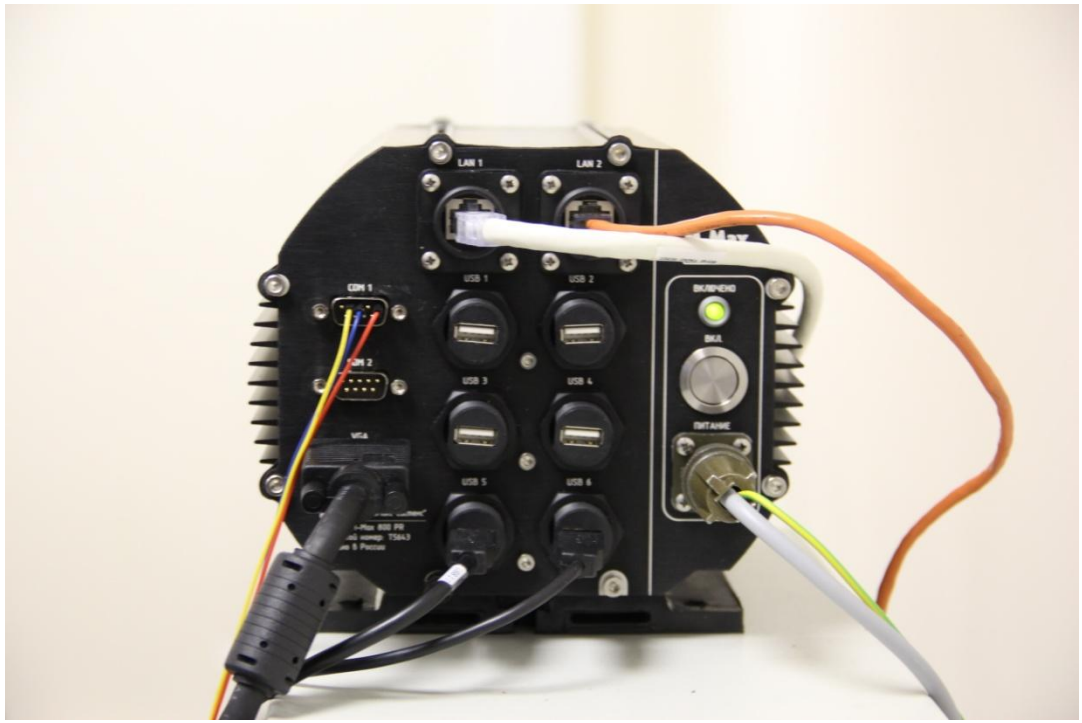
Интегрированные решения затрагивают и стратегии адаптации к новым платформам и условиям применения, с возможностью настраиваемых систем кодогенерации.

Управляющее ПО для беспилотных летательных аппаратов

А. В. Ширяев, Егорьевский филиал АО «НЦПЭ»

Система аварийной регистрации параметров САРП РоАЭС-1

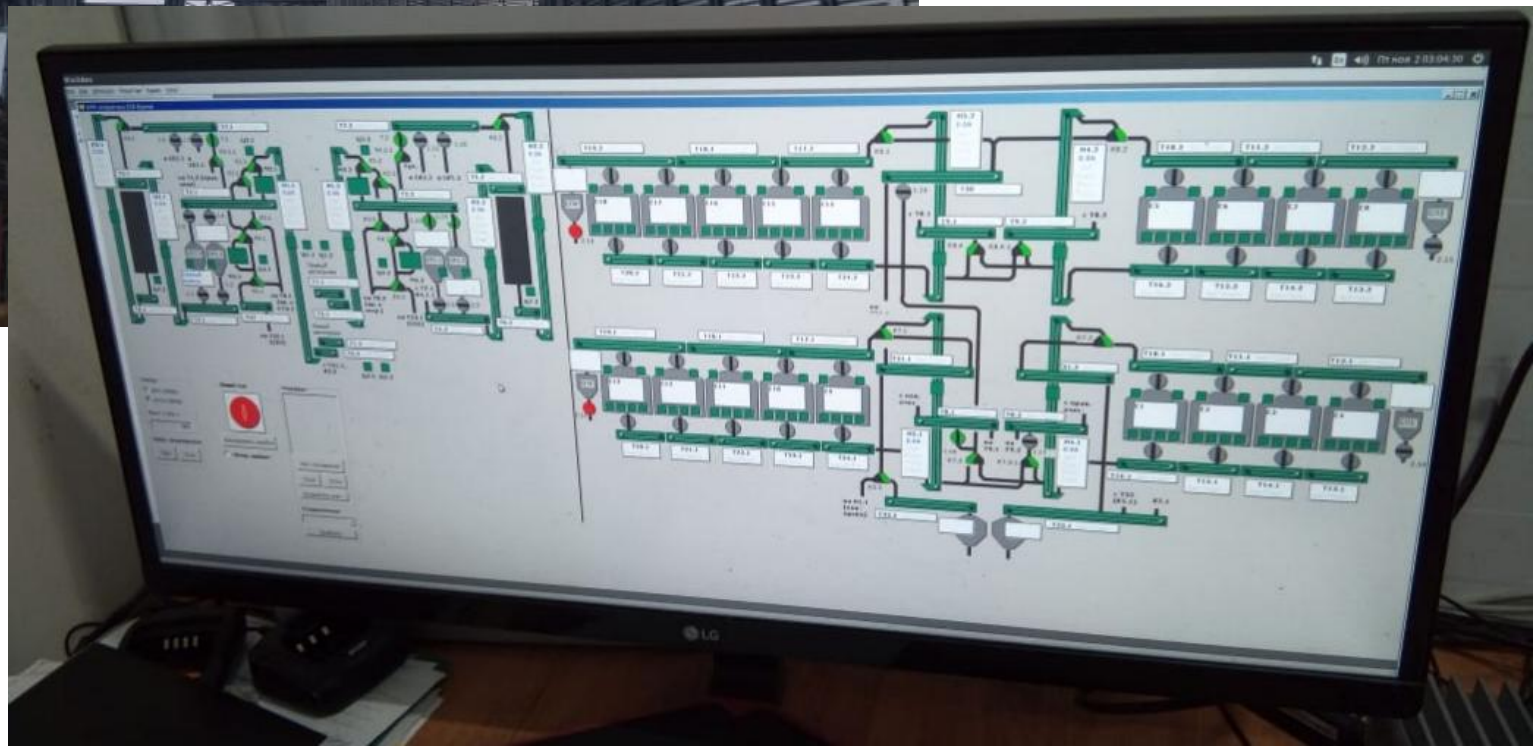
- В промышленной эксплуатации с 2014 г.;
- Переносимый рантайм как на стандартную ОС, так и на микро-ОС (ядро, планировщик) на основе A2 поверх голого железа;
- Разработано специализированное коммуникационное ПО.



АСУТП в агропроме

- И. Е. Ермаков (Ermakov Systima)
- Элеваторы холдинга «МираТорг». На платформе ERSY Control (SCADA + рантайм управления на базе ОС Linux)
- Component Pascal и BlackBox
- Современные SCADA – графика на базе браузерных движков, часто – Flash и т.п.
- BlackBox – кроссплатформенная компонентная графика, < 20 Мб исполняемая сборка SCADA

АСУТП в агропроме



Задачи научных расчетов повышенной сложности

- Программа для обработки данных научной установки ИЯИ РАН «Троицк ню-масс», в результате получена лучшая в мире оценка массы нейтрино. До того в течение 10 лет данные обрабатывались на программах на фортране с использованием библиотек ЦЕРНа и наблюдалась загадочная аномалия, которая обсуждалась в Президиуме РАН и на телевидении;

- Программа для класса задач компьютерной алгебры в физике элементарных частиц, с помощью которой выполнены уникальные по сложности расчёты, позволившие устранить 10-летнее рассогласование теории и эксперимента в распадах b-кварка. Конкурирующая программа была написана на Си++, программа на Обероне была написана в 12 раз быстрее и работала в 8 раз быстрее.

Оберон имеет исключительную родословную (Гуткнехт 10/2018)

Год	Язык	Концепции
1955	ALGOL/68 ALGOL/W	Процедуры
1970	Pascal	Безопасная типизация, программирование небольших задач
1980	Modula-2	Модули и интерфейсы, программирование больших задач
1990	Oberon	Объектно-ориентированное программирование, расширение типов
2000+	Active Cells	Гибридное программирование, описание железа

Достигнув Оберона, авторы-основатели (Вирт, Гуткнехт) переключились на смежные области - ПЛИС.

Отечественная школа компиляторов

Цель программиста, как создание интеллектуально-управляемых программ (Э. Дейкстра) достигается только при полном контроле над ОС и компиляторами.

Простота и строгость Оберона

Строгость обеспечивает отсутствие связанных с языком уязвимостей в части переполнения за счет:

- Строгой корректности операций с основными и расширенными типовами;
- Полного контроля указателей, массивов, стека;
- Компиляторов и генераторов кода отечественной разработки.

Простота “As Simple as Possible but not Simpler” обеспечена полным исключением проблемных решений за более, чем 40-летнюю историю развития от предка Паскаля.

Проблема избыточной сложности

- Избыточно сложным стекам доверять нельзя
- Оберон-сообщество имеет свой взгляд на проблему качества ПО. В чём причины?
- Асимметрия информации на рынке технологий (ухудшающий рыночный отбор по Аккерлофу)
- Возникновение самоподдерживающихся «пищевых цепочек» вокруг коммерческих технологий
- Нарушение принципа Парето, наслаивающееся на каждом уровне, даёт экспоненциальный рост?
- Теорема мат. логики о росте длины доказательства в башню экспонент раз, при неудачной декомпозиици
- Традиция критической мысли в ИТ: Дейкстра, Хоар, Вирт
- Считали, что разрыв порочных кругов возможен из академической среды

Достаточно ли только открытости?

- Открытость без простоты не даёт качества и доверия. Можем ли доверять GCC или ядру Linux? Сколько лет жили закладки во FreeBSD?
- Оберон-сообщество: ценности открытости + ценности простоты. Обозримые, полностью подконтрольные технологические стеки, построенные по Парето (20% кода обеспечивают 80% функциональности, остальное - «от лукавого»)
- Понимание и преодоление близорукости рынка (асимметрии информации, ловушек «локальных оптимумов» и др.)

Стратегия инструментов разработки

- На конференции «Оберон-технологии, образование и проблема качества в цифровой индустрии» частью участников продвигалась концепция развития предметно-ориентированных (в том числе визуальных) технологий, построенных не как «чёрные ящики», а над стеком «Простой и надёжный язык – предметно-ориентированный ООП-фреймворк – CASE/DSL/4GL над его абстракциями»