Перспективы Оберон-технологий для стратегических отраслей

Дагаев Дмитрий Викторович,

Главный Эксперт,

АО «Русатом Автоматизированные системы управления»

Консультант проекта Информатика-21,

Microsoft Certified Solution developer,

dvdagaev@yahoo.com

Путь извилист, но перспективы светлые

Футурология «от отрицания» via negativa может достоверно говорить о будущих событиях только в негативном ключе:

- Финансовый кризис и кризис ответственности;
- Торговые войны в глобальном масштабе;
- Рост числа проблем в части кибер-безопасности.

У глобальных корпораций нет никаких причин использования Оберонов: базовые идеи, носители и патентованные продукты (C/C++/C#, Java , Go) разрабатывались или переместились в США и управляются крупным бизнесом.

Глобальный рост рынков далее невозможен, возможна только переориентация локальных рынков стран (Китай, ЕС, РФ), готовых взять на себя ответственность за создание ***интеллектуально-управляемых программ*** по Э.Дейкстре, предложив лучшие решения в части надежности и киберзащищенности.

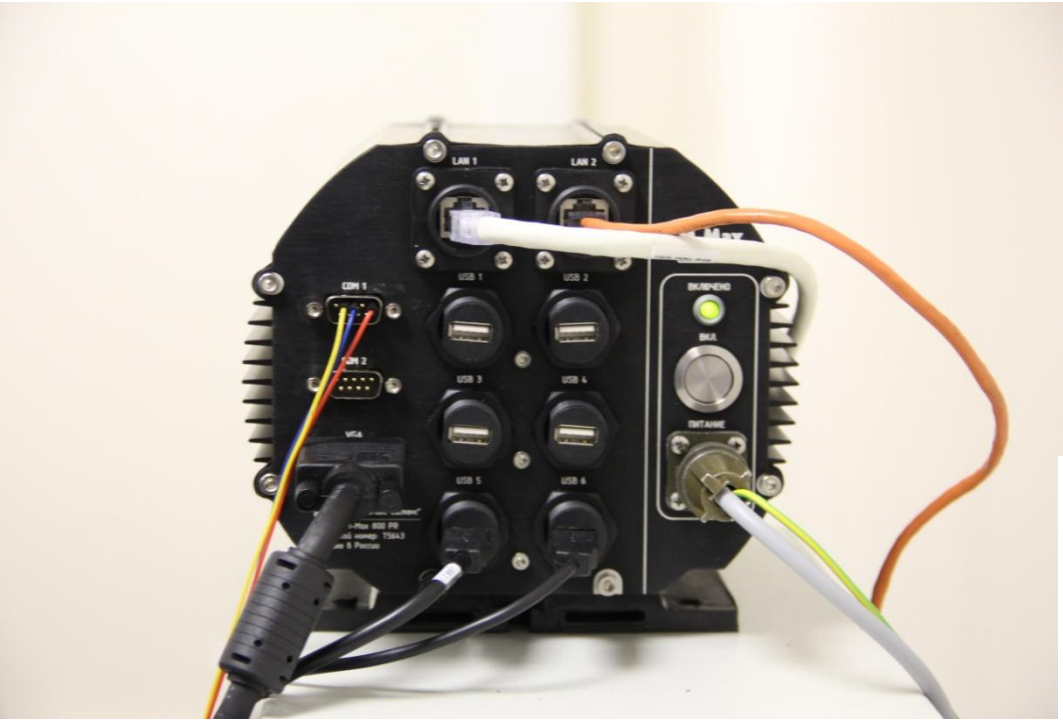
Смогут ли национально-ориентированные корпорации использовать открывающиеся возможности? Оберон-технологии имеют научно-техническую и методическую основу для создание такого полного цикла ПО. Но смысл пути предполагает наличие ресурса воли, а не использование локомотива американской экономики, как это происходит сейчас.

Кросс-платформенное ПО

Отказ по общей причине common cause failure CCF – используемое в промышленных стандартах понятие единичного события, приводящего к отказу всей системы.

Диверсификация или принцип разнообразия используется как основной способ борьбы с CCF.

В плане жизненного цикла систем адаптация означает возможность развития с целью приспособления к событиям CCF.



Система PAMS «черный ящик» (на основе BlackBox/XDS) успешно функционирует на 1 э/б РоАЭС с 04.2014. Но есть вопросы (черные лебеди) :

64 bit, ARM и другие;

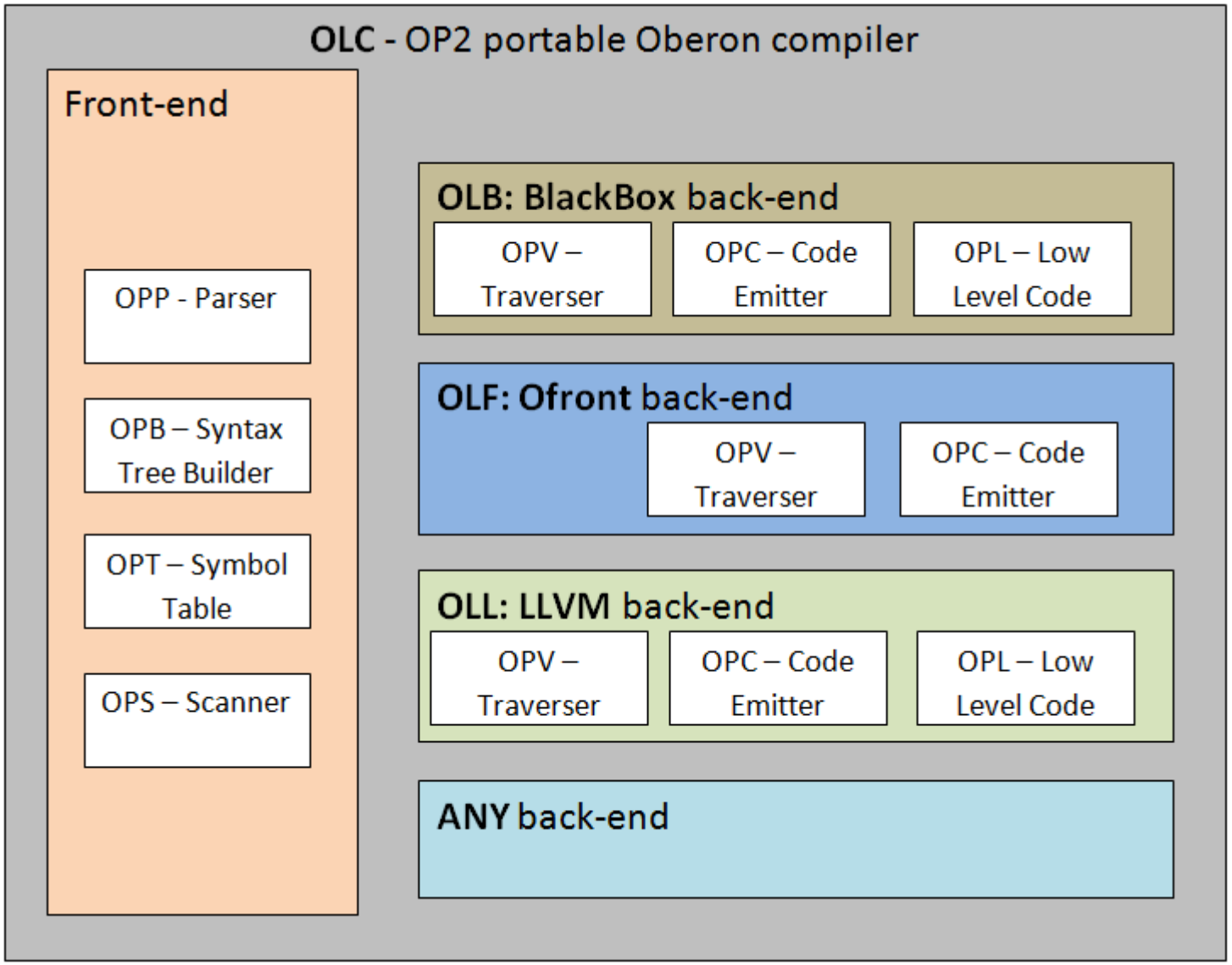
Другие ОС: Astra Linux, QNX.

Oberon-L Compiler

Исправление (ректификация) имен (чжэнмин, кит. 正名 *zhèngmíng)*, Oberon-L вместо CP.

OP2 компилятор (Regis Crelier) со сменными бэкендами:

- BlackBox back-end;
- Ofront back-end;
- LLVM back-end;
- Иной back-end.



Диверсификация для разных платформ и ОС

	OLB - BlackBox	OLF - Ofront	OLL - LLVM
32 бит	YES	YES	YES
64 бит	NO	YES	YES
ARM	NO	YES	YES
Загрузка модулей	YES	NO	YES
Astra Linux	NO	YES	NO?
QNX	NO	YES	NO?

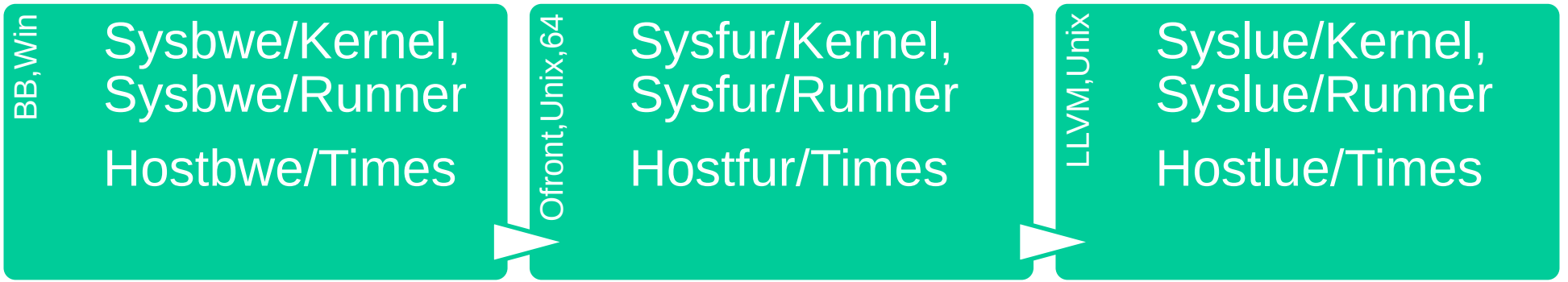
Конструкция OLC-компилятора со сменными бэкендами позволит осуществить покрытие всех основных программных и операционных платформ.

Бэкенды разнообразны по принципам работы: нативный код (OLB - BlackBox), транслятор в C (OLF - Ofront), LLVM-код виртуальной машины (OLL - LLVM). В двух последних случаях применяются оптимизирующие компиляторы.

Конструкция OLC предполагает возможность последующего добавления бэкендов, например, для встроенных систем.

Единый фронтенд обеспечивает входную совместимость компилируемых программ.

Структурная реализация




```
MODULE OltestDateTime;
   IMPORT Runner, Times, HostTimes;
   PROCEDURE Run*;
    VAR t: Times.Time;
   BEGIN
    t := Times.GetTime();
   END Run;
BEGIN
   Runner.SetRun(Run)
END OltestDateTime.
```

Кроссплатформенность реализуется сборкой с разными файлами, ядрами:

- Sysbwe/Kernel, Runner и Hostbwe/Times для случая BlackBox, Win;
- Sysfur/Kernel, Runner и Hostfur/Times для Ofront, Unix, 64бит;
- Syslue/Kernel, Runner и Hostlue/Times для LLVM, Unix.

МЭК 60880 - надежное встроенное ПО

МЭК 60880 определяет требования к наиболее критически важным системам для АЭС, выполняющих функции категории А.

В части ОС идеальный конечный результат - ОС нет, а функции ее выполняются:

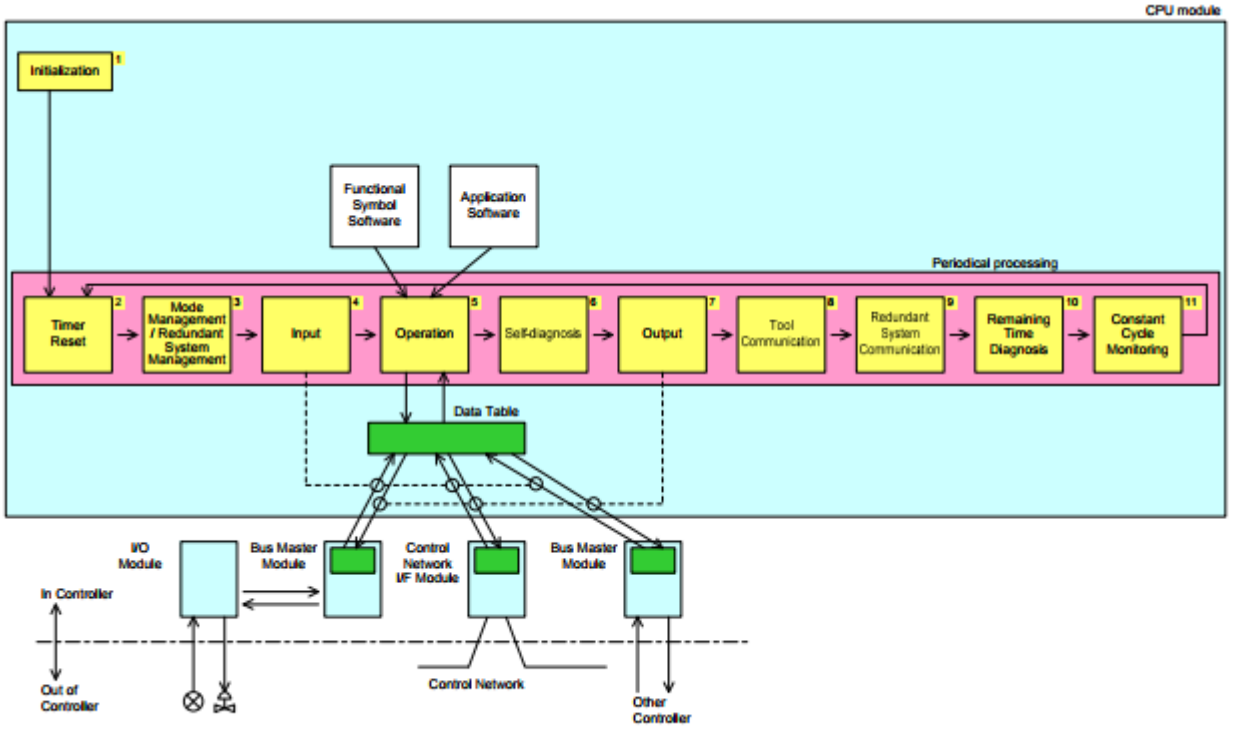
- B.2cb Следует избегать использования универсального операционного программного обеспечения (операционных систем);
- B.2cc Если операционная система необходима, то ее применение следует ограничить небольшим числом простых функций;
- B.2cd Операционная система должна содержать только необходимые функции.

Системы строят обычно на ПЛИС или без ОС с аппаратным циклом от таймера.

Идеальное управление задачами - отсутствие планировщика, в одном потоке от таймера. Идеальная структура программы - без ветвлений, с жестко заданными ограничениями итераций циклов, с постоянным числом принимаемых сигналов.

- B.2dd Время прогона не должно существенно изменяться в результате изменения входных данных;
- B.2de Значение изменения времени прогона, которое может быть вызвано входными данными, должно быть документально оформлено;
- B.2dg Объем данных, считываемых в течение одного вычислительного цикла, должен быть постоянным.

Реализация MELTAC – Mitsubishi Electric Corporation



Система периодически работает по таймеру. Основной цикл занимает не более 80% CPU. Если больше, срабатывает диагностика, приводящая к рестарту. Реализует МЭК 60880.

Проблема систем РВ – ***Время прогона*** должно быть ограничено.

Ограничение времени прогона

Требования в части компилятора по циклам и массивам оставляют только циклы FOR с возможным выходом по отказу, условие CASE – ELSE исключается:

- B.4ac Следует избегать переходов из циклов, если они не ведут к полному окончанию цикла. Исключение - выход по отказу;
- B.4af Концепция "вариант по умолчанию" должна быть зарезервирована для обработки сбоя;
- B.4ag Следует использовать циклы только с постоянными максимальными областями значений переменной цикла.

```
FOR j := 0 TO N-1 DO

 IF in.value[j].quality = Q_BAD_COMM THEN EXIT END

END
```

Реализация требований 60880 приводит к ***требующему адаптации диалекту Оберона***, в котором ряд операторов (NEW, WHILE, LOOP, REPEAT) отключены или ***добавлены анти-свойства –NEW –WHILE –LOOP -REPEAT***.

USE – Инициатива добавления гарантий использования

USE предлагается как ключевое слово, уведомляющее фронтенд о дезавуировании или использовании определенного оператора для данной версии программного кода. Операция ‘–’ отключает операторы, ‘+’ восстанавливает отключенные, а ‘*’ ограничивает их использование заранее определенным образом.

Для адаптированного для стандарта 60880 потребуется нижестоящее определение и вариант бэкенда, который это поддерживает. Отключаем `NEW, WHILE, LOOP, REPEAT, CASE/ELSE`.

```
USE –NEW –WHILE –LOOP –REPEAT –ELSE(CASE) +EXIT(FOR);
```

Использование USE может создать диалект, близкий Оберону-07 в существенных частях:

```
USE –LOOP *CASE *RETURN –SHORTINT –LONGINT +ELSIF(WHILE)
```

При этом ограниченный CASE предполагает только целые варианты, а ограниченный RETURN – только как последняя строка функции.

Ограничение динамической памяти

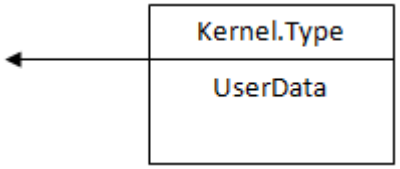
В системах жесткого реального времени обычно применяется *статическое распределение памяти*.

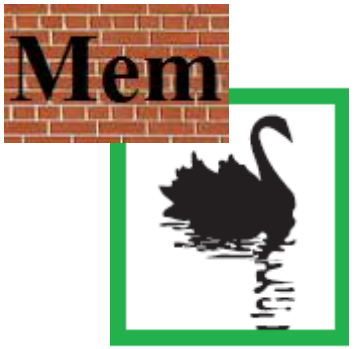
```
USE -NEW;
```

Если динамическая память `NEW` все же используется, ее можно отключать после инициалицации:

```
Kernel.DisableHeap();
```

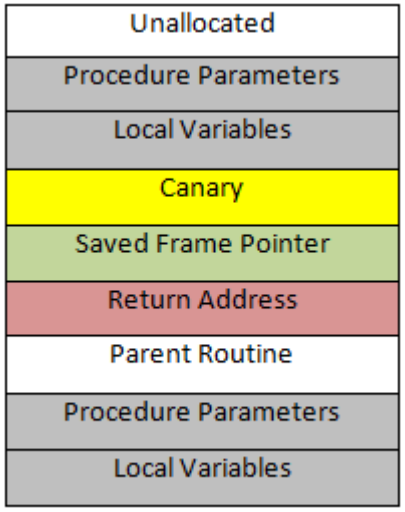
Если динамическая память используется ограниченно, можно отключить сборщик мусора и реализовать и вставлять в ядро свой менеджер памяти, передающий ссылки на статические структуры с предустановленными типами:





Иначе у вас вряд ли система жесткого реального времени.

Защита от переполнения буфера



Из-за присущих C/C++ проблем с негарантированной типизацией и размерами массивов широкое распространение получили уязвимости, основанные на атаках переполнении стека. Решение с «канарейкой» не гарантирует спасения.

Оберон-технологии гарантируют:

- Проверку типизации объектов при копировании;
- Проверку индексов массивов при копировании.

```
USE –SYSTEM –PROCEDURE(TYPE);
```

Требуется гарантия отключения системного модуля и процедур обратного вызова (callback).

Наиболее жесткие требования РД 1кл НСД требуют записи маскирующей информации в освобождаемую (в том числе, и стековую) память. Для этих целей дорабатывается бэкенд компилятора.

Расширение активными объектами

Для реализации многопоточности возможно движение в сторону отработанных решений ActiveOberon. Добавляем в Oberon-L сущности, относящиеся к активным объектам.

```
Object = POINTER TO RECORD
    s: Synchronizer;
    fin: BOOLEAN;
    time, pretime: LONGINT
END;

PROCEDURE [safe] (o: Object) ACTIVITY;
BEGIN
    LOOP
        BEGIN [exclusive]
            AWAIT(s.fin OR (s.time # s.pretime));
            IF s.fin THEN EXIT END;
        END;
        s.o.Wakeup;
    END
END ACTIVITY;
```

Расширение активными объектами добавляет 4 ключевых слова в компилятор: `ACTIVITY, AWAIT, [exclusive], [safe]`. Бэкенд и ядро должны поддерживать добавленную функциональность.

Время собирать камни

МЭК880 -9 удалить, *4 изменить, Oberon07 -5 удалить *3 изменить,

Oberon-L эталонный набор слов, Active Oberon-L +4 добавить.

ABSTRACT
ARRAY
BEGIN
BY
CASE
CLOSE
CONST
DIV
DO
ELSE
ELSIF
USE
EMPTY
END
EXIT
EXTENSIBLE
FOR
IF
IMPORT
IN
IS
LIMITED
LOOP
MOD
MODULE
NEW
NIL
OF
OR
OUT
POINTER
PROCEDURE
RECORD
REPEAT
RETURN
THEN
TO
TYPE
UNTIL
VAR
WHILE
WITH

ABSTRACT
ARRAY
BEGIN
BY
CASE
CLOSE
CONST
DIV
DO
ELSE
ELSIF
USE
EMPTY
END
EXIT
EXTENSIBLE
FOR
IF
IMPORT
IN
IS
LIMITED
LOOP
MOD
MODULE
NEW
NIL
OF
OR
OUT
POINTER
PROCEDURE
RECORD
REPEAT
RETURN
THEN
TO
TYPE
UNTIL
VAR
WHILE
WITH

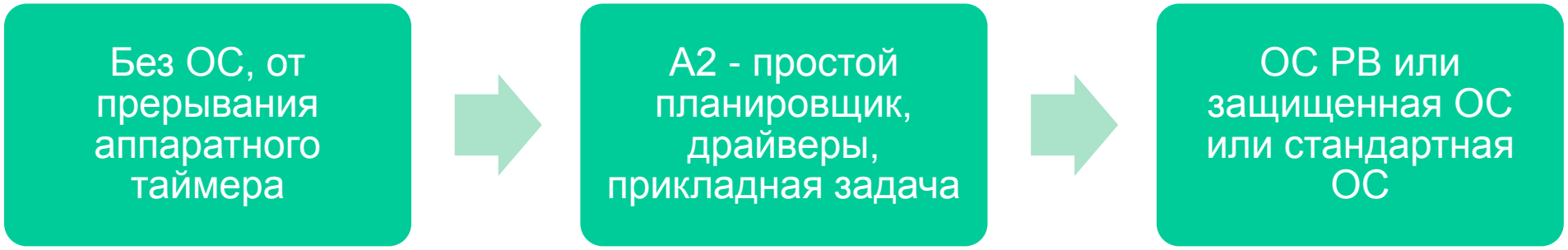
ABSTRACT
ARRAY
BEGIN
BY
CASE
CLOSE
CONST
DIV
DO
ELSE
ELSIF
USE
EMPTY
END
EXIT
EXTENSIBLE
FOR
IF
IMPORT
IN
IS
LIMITED
LOOP
MOD
MODULE
NEW
NIL
OF
OR
OUT
POINTER
PROCEDURE
RECORD
REPEAT
RETURN
THEN
TO
TYPE
UNTIL
VAR
WHILE
WITH

ABSTRACT
ARRAY
BEGIN
BY
CASE
CLOSE
CONST
DIV
DO
ELSE
ELSIF
USE
EMPTY
END
EXIT
EXTENSIBLE
FOR
IF
IMPORT
IN
IS
LIMITED
LOOP
MOD
MODULE
NEW
NIL
OF
OR
OUT
POINTER
PROCEDURE
RECORD
REPEAT
RETURN
THEN
TO
TYPE
UNTIL
VAR
WHILE
WITH
AWAIT
ACTIVITY
[safe]
[exclusive]

Двустороннее масштабирование

Очень существенным представляется демасштабирование, при котором при сокращении объема функциональности увеличиваются показатели надежности и защищенности используемых решений.

Горизонтальное масштабирование



В плане диверсификации Оберон-решений для разных платформ важно отметить также горизонтальное масштабирование. Одно и то же решение может быть реализовано в разных средах исполнения.

Самая простая программа более портабельна, и, шире, более простые формы адаптируются в большем диапазоне окружающей среды.

Вся линейка решений позволит наилучшим способом выбрать подходящие средства для реализации систем в стратегических отраслях с сохранением во всех вариантах присущих Оберонам гарантий киберзащищенности.

Вопросы и Приложения

Пояс Оберона

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

Приложение1 – Процедуры Таймера

```
MODULE OltestDateTime;
    IMPORT Runner, OLog, Times, HostTimes;
    PROCEDURE Run*;
     VAR t: Times.Time; st: Times.SystemTime; s: ARRAY 128 OF CHAR; res: INTEGER;
    BEGIN
     t := Times.GetTime();
     OLog.String("Time="); OLog.Int(t); OLog.Ln;
     OLog.String("sec="); OLog.Int(Times.ToSec(t));
     OLog.String(" mcs="); OLog.Int(Times.ToMcs(t)); OLog.Ln;
     Times.ToSystemTime(t, st, res); Times.SystemTimeToString(st, Times.tDATETIME, s);
     IF res # 0 THEN OLog.String(" ?") END; OLog.String(" UTC="); OLog.String(s); OLog.Ln;
     Times.ToLocalTime(t, st, res); Times.SystemTimeToString(st, Times.tDATETIME, s);
     IF res # 0 THEN OLog.String(" ?") END; OLog.String(" Local="); OLog.String(s); OLog.Ln;
     Times.Sleep(Times.FromSecMcs(0, 300000, FALSE));
     t := Times.GetTime();
     OLog.String("After Sleep(0.3sec) Time="); OLog.Int(t);  OLog.Ln;
    END Run;
BEGIN
    Runner.SetRun(Run)
END OltestDateTime.
```

Приложение 2 – МЭК 60880

B.2cb Следует избегать использования универсального операционного программного обеспечения (операционных систем)

B.2cc Если операционная система необходима, то ее применение следует ограничить небольшим числом простых функций

B.2cd Операционная система должна содержать только необходимые функции

B.2dd Время прогона не должно существенно изменяться в результате изменения входных данных

B.2de Значение изменения времени прогона, которое может быть вызвано входными данными, должно быть документально оформлено

B.2dg Объем данных, считываемых в течение одного вычислительного цикла, должен быть постоянным

B.2e Необходимо ограничивать применение прерываний

B.2ea Прерывания могут использоваться, если они упрощают проект ПО и не делают верификацию чрезмерно сложной

B.2ed Если прерывания используются, то для непрерываемых частей необходимо иметь оценки максимального времени вычислений, чтобы можно

было рассчитать максимальное время, в течение которого прерывание запрещено

B.3c Содержимое памяти должно быть защищено или контролироваться

B.3db Следует проверять правильность передачи любого параметра, включая проверку типа параметров

B.3dc При адресации массива следует проверять его границы

Приложение 3 – UseIEC880

```
MODULE UseIEC880;

   (* Operators *)

   USE -WHILE, -LOOP, -REPEAT, -WITH, -UNTIL, -CLOSE, -OUT,

    +EXIT(FOR),          (* Loops with constant maximum loop variable ranges *)

    -ELSE(CASE), (* The concept of a “default branch” reserved for failure handling*)

    -PROCEDURE(PROCEDURE), (* recursive structures and code compaction avoided *)

    *RETURN(PROCEDURE);  (* Branches out of loops should be avoided,

                if they do not lead exactly to the end of the loop *)

   (* Identifiers *)

   USE  -ANYPTR, -ANYREC, -ABSTRACT, -EXTENSIBLE, -LIMITED, -EMPTY, -INF, -SYSTEM,

    -LONG, -SHORT, -NEW;


END UseIEC880.
```

Приложение 4 - Многозадачность кооперативная/вытесняющая

Рабочие станции могут объединять в рамках одного приложения несколько задач с ***ограниченным временем прогона***, управляемым планировщиком.