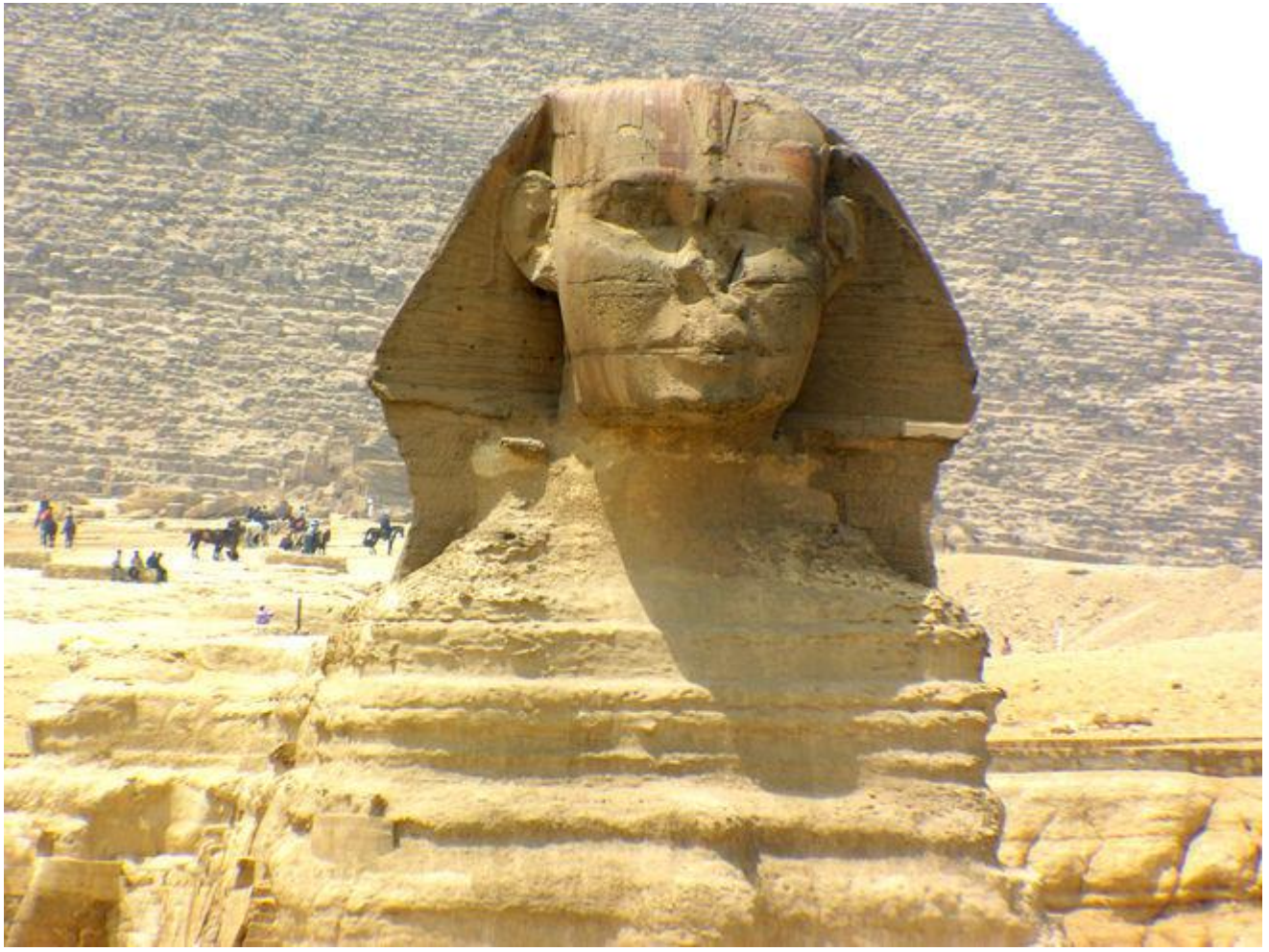
# О разработке среды исполнения Оберон-системы с заданными свойствами эргодичности

Дагаев Дмитрий Викторович,
От проекта Информатика-21,

Место Работы:
АО «Русатом Автоматизированные системы управления»,
Главный Эксперт

# Улыбка Сфинкса



Иероглифы, начертанные на базальтовой скале Абу-Симбела в Египте:

“Когда человек узнает, что движет звездами, Сфинкс улыбнется и Мир исчезнет”.

A problem has been detected and Windows has been shut down to prevent damage to your computer.

This is probably not the first time you've seen this stop error, as you've probably wrecked a computer before.

A problem has been detected and Windows has been shut down to prevent damage to your computer.

This is probably not the first time you've seen this stop error, as you've probably wrecked a computer before.

I would tell you to run a system diagnostic utility, run a memory check, or check for faulty or mismatched memory, but if you're reading this, I'm pretty sure you don't know how to do any of those things.

You are also probably using a shitty anti-virus program like AVG free edition with no rootkit detection capabilities, and I guarantee you've never heard of Malwarebytes, SUPERAntiSpyware, or any other anti-malware program. I'd be willing to bet that you don't use Firefox with WOT and AdBlock Plus either.

If this is a laptop I'm pretty positive you've either dropped it a few times or spilled a drink on it.

Windows updated? Didn't think so.

Well, you could try to restart in Safe Mode by tapping F8 at bootup, but that's more than likely not going to work...you're just going to see this again. Even if it does work, you'll be lost as to what to do next.

You could reinstall your Operating System, but I know you either didn't get a disk when you bought this computer, or more realistically, you lost it.

Well, here's the obligatory Technical Information, but it will be of no use to you:

*** STOP: 0x0000008D (0x0000007E, 0x0000005b, 0x0000008a, 0x0000003c)

Collecting data for crash dump ...
Initializing data for crash dump ...

# Об эргодичности

- Свойство эргодичности означает стационарность, вероятности αi состояний системы не зависят от времении и не зависят от распределения вероятностей в начальный момент времени, то есть: αi=const;
- При отсутствии эргодичности математическое ожидание по временным рядам (временная вероятность) не совпадает с математическим ожиданием по пространственным рядам (ансамблевая вероятность):
  - O.Peters, M. Gell-Mann Evaluating gamples using dynamics, 2016;
  - O.Peters The ergodicity problem in economics, 2019.
- Компьютерное моделирование игры в русскую рулетку (Н.Талеб) с 1 патроном из 6 и призом в 1 млн $ дает:

- средний выигрыш в $833333 в N серий из 1 попытки;

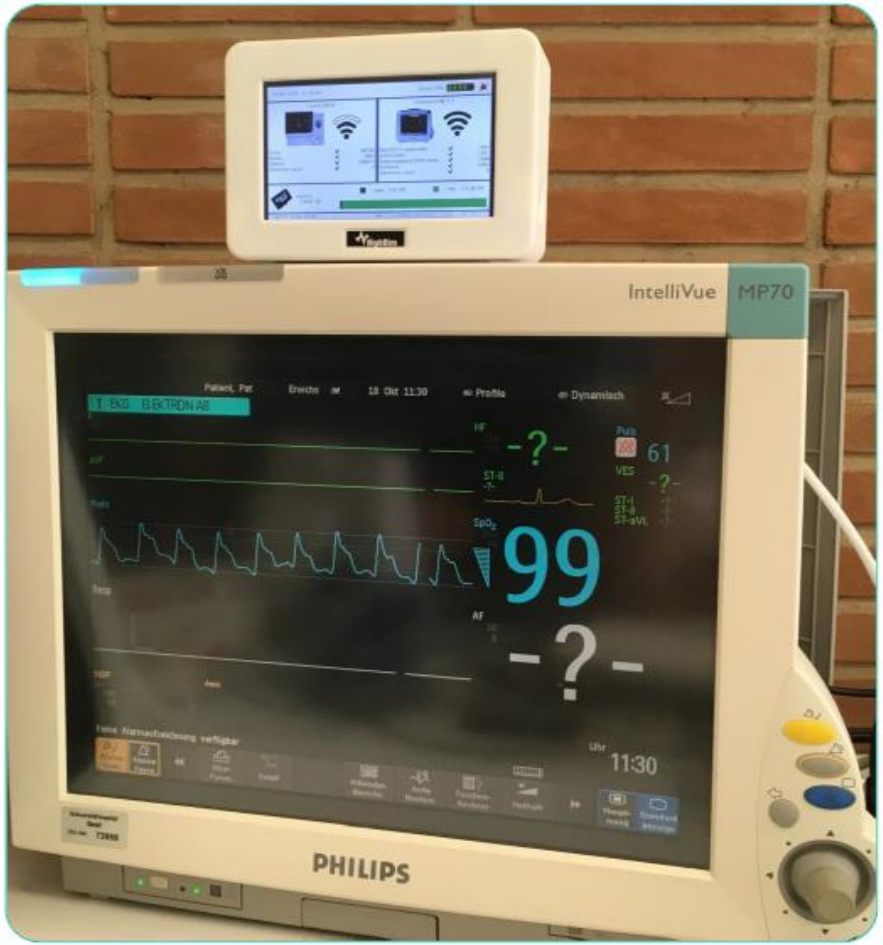
- аварийное завершение без возможности восстановления при N попытках (улыбка Сфинкса).

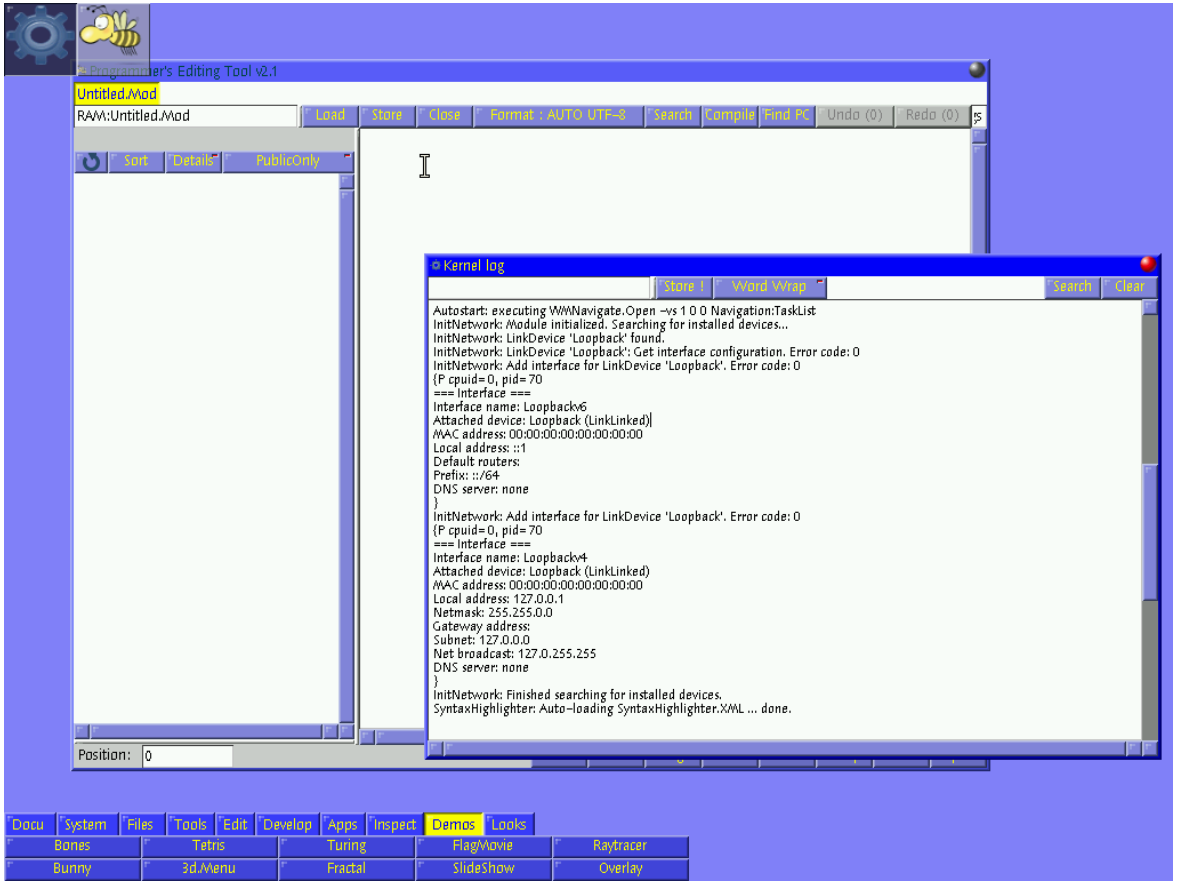
А как разработать ПО с предсказуемым состоянием?

И какие свойства должны соответствовать понятию эргодичности?

# Active Oberon система A2

Active Oberon системы A2 https://github.com/metacore/A2OS. A2 представляет собой однопользовательскую многозадачную систему, которая может работать поверх bare metal или POSIX OS. Область применения – промышленные встроенные надежные системы реального времени (swiss quality).



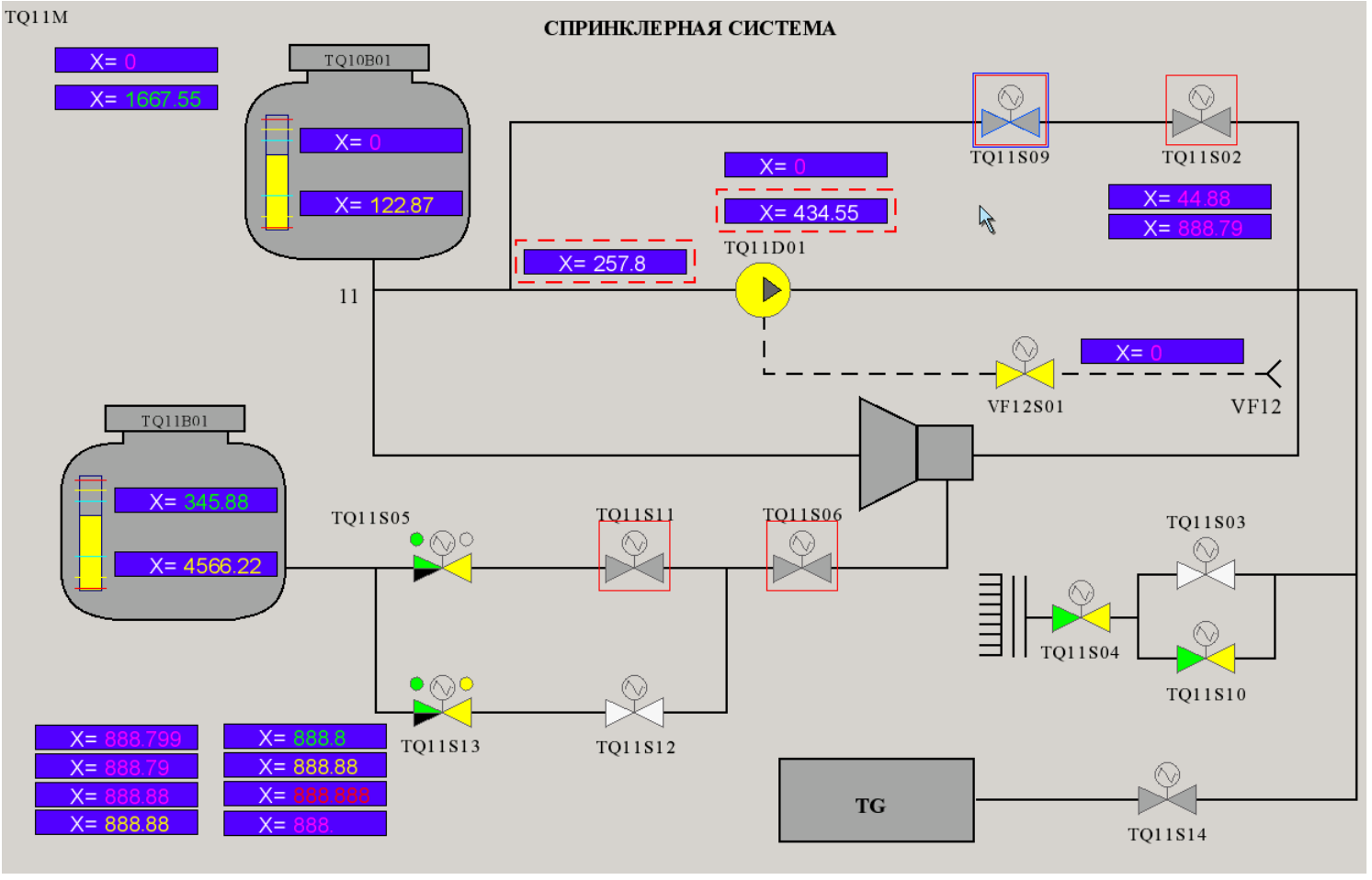



# Среда исполнения ДСКУ на основе A2

ДСКУ разрабатывалась для использования в системах безопасности для реализации функций категории А МЭК 60880, для которых невозможно использовать стандартные ОС и компиляторы.

Рантайм ДСКУ реализован существенной переработкой минимального подмножества A2 под заявленные требования.

Прототип для использования во встроенных устройствах с/без ЧМИ.



# Допущение #1: Представление о неограниченности памяти

1. Отсутствуют утечки памяти;
2. Нет проблемы фрагментации динамической памяти;
3. Динамически запрашиваемая память всегда будет выделена;
4. Идеальное срабатывание сборщика мусора за нулевое время;
5. Отсутствует ограничение по размеру стека;
6. Идеальная надежная работа своппинга за нулевое время;
7. Постраничная организация памяти не оказывает воздействия на функционирование системы во времени;
8. При рестарте компонентов системы гарантируется выделение им статической памяти.

```
using namespace boost;
property_tree::tree pt;
property_tree::read_xml("Name.xml", pt);
```

Последовательность обрабатывается корректно до появления файла нестандартно большого объема вызывающего исключения.

Варианты:

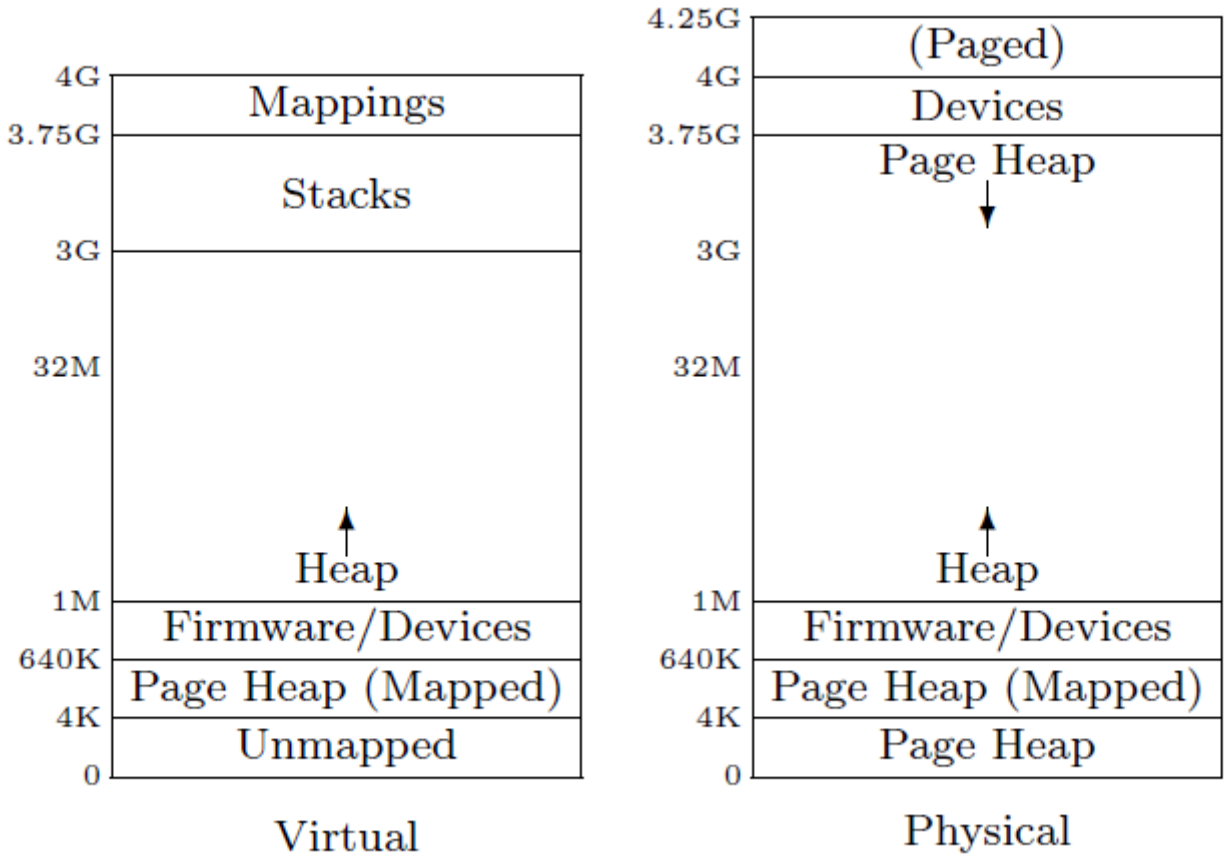
1. исключение не обработано – аварийное завершение;
2. исключение обработано – потеря значимой информации.

# Модель памяти A2 и управление памятью

A2 использует механизмы сегментации, при этом динамическая виртуальная память отображается на физическую с сохранением адресов. Наращиваемая стековая память предоставляется активным объектам.

#1.6 Наличие отсутствия своппинга.

#1.7 Отсутствует воздействие постраничной организации на систему.



# Запрет управления памятью после фазы инициализации

Этап 1 – Загрузка системы;

Этап 2 – Инициализация. Объектам и данным предоставляется динамическая память. Выделение запрашиваемой стековой памяти (рекурсия отсутствует);

**Этап 3 – Запрет выделения памяти, отключение сборщика мусора, запрет дисковых операций;**

Этап 4 – Код старта активных объектов;

Этап 5 – Цикл обновления по таймеру;

Этап 6 – Окончание работы и перезагрузка.

Программное восстановление – этап 4, далее этап 5.

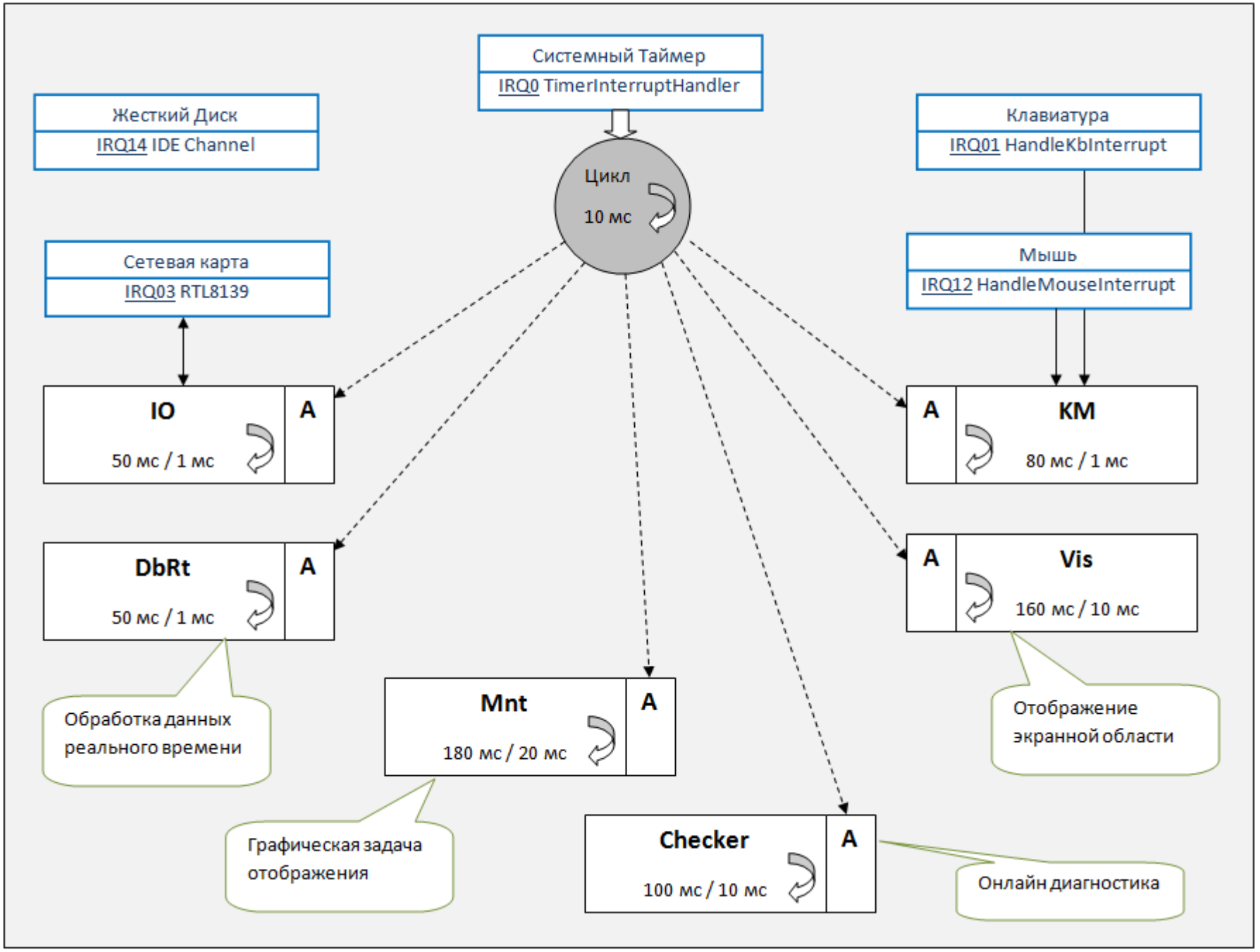
#1.1 - #1.5, #1.8 Полностью детерминированная работа с памятью, доказывающая свойство эргодичности в части использования памяти.

# Допущение #2: Реальное время и синхронизация

1. Отсутствуют deadlock;
2. Нет гонок race conditions и вызванных ими искажений критически важных данных;
3. Время прохождения сигнала через систему (латентность) фиксировано с известной точностью;
4. Непосредственное взаимное влияние процессов (активностей) друг на друга отсутствует;
5. Прерывания системы ввода/вывода не оказывают влияния на процессы обработки.

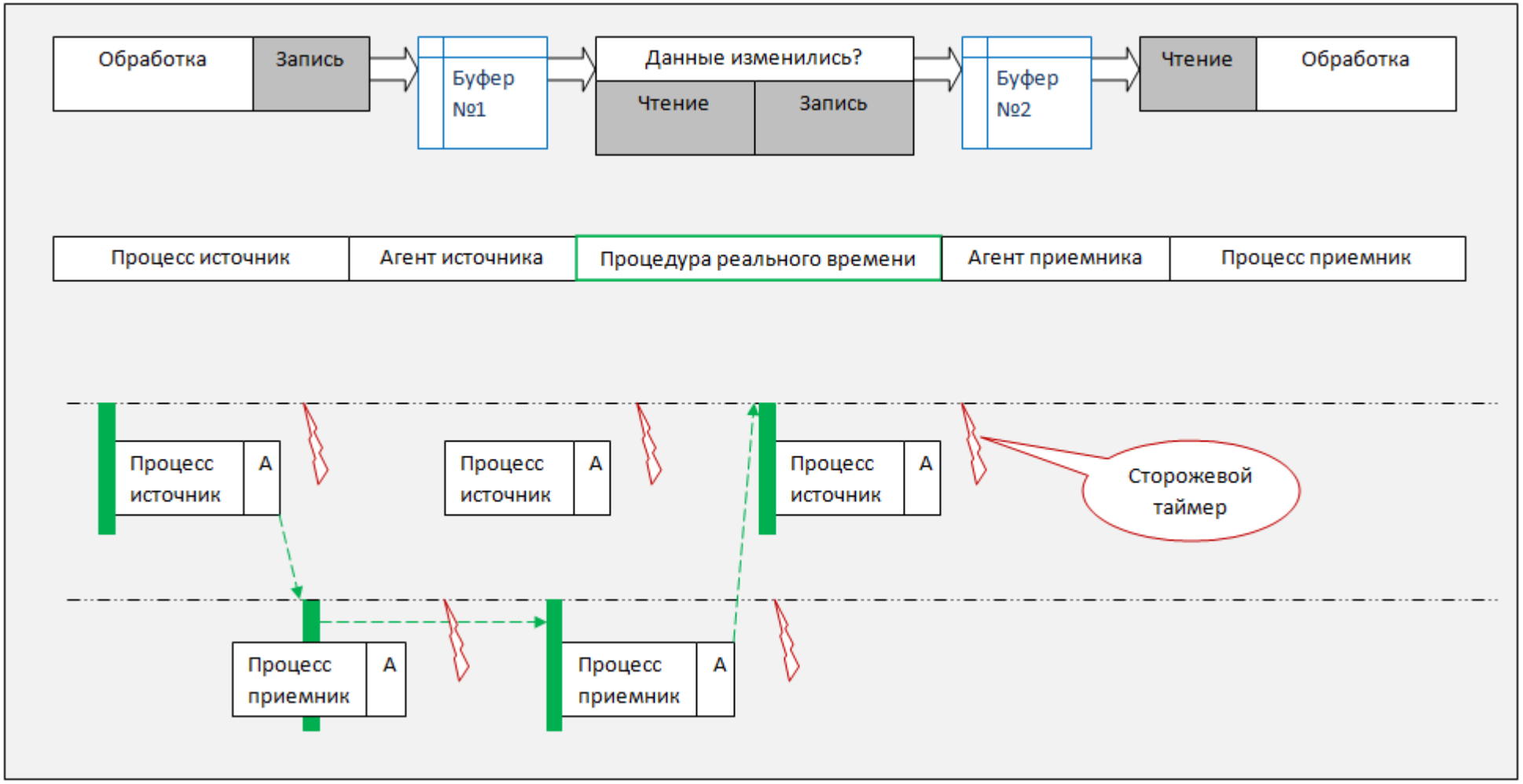
Требуются доказательства отсутствия неэргодичности взаимодействия.

# Активные объекты и синхронизация



# Межзадачный обмен посредством двойной буферизации

Неблокирующее взаимодействие между объектами осуществляется по схеме ЧтениеВходного-Обновление-ЗаписьВыходного буфера с {REALTIME} атомарным обменом буферов за фиксированное время.



# Гарантии реального времени

#2.1, #2.2 Отсутствие блокировок гонок – нет и ожидания и взаимного доступа к данным, только атомарный обмена буферов за фиксированное время;

#2.3 Время прохождения сигнала обеспечивается сторожевым таймером, при овертайме – рестарт компонента;

#2.4 Активные объекты не взаимодействуют, а только через агенты, работающие с буферами;

#2.5 Дисковая система отключена, **число прерываний графических устройств ограничено за интервал** (заметна неравномерность движения трекбола). Сетевое взаимодействие реализовано на основе UDP с планами перевода на полевые сети на основе механизма поллинга.

Неполная гарантия эргодичности RealTime с перспективой обеспечения в будущем.

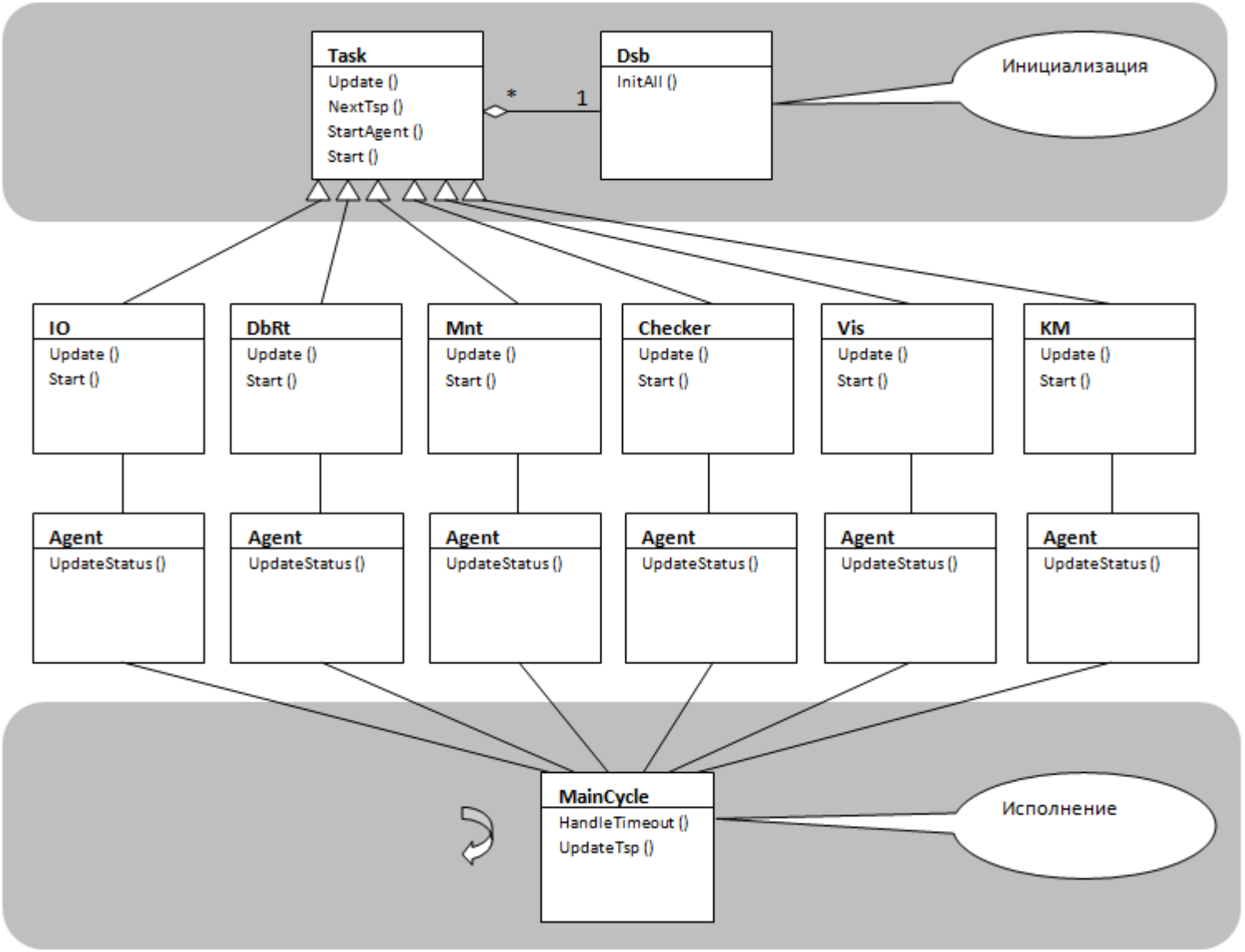
# Допущение #3: Исключения и восстановление

1. Исключения не приводят к потери ресурсов;
2. Обработка исключения не приводит к генерации исключения внутри обработчика;
3. Восстановление после обработки исключения всегда завершается успешно;
4. Восстановление приводит к работоспособному состоянию, близкому к состоянию первого старта;
5. Объект с исключением не оказывает влияние на работоспособность других объектов.

Требуются доказательства отсутствия неэргодичности исключений, их обработки и восстановления.

# Агенты активных объектов

Активные объекты создаются на этапе инициализации. Активные объекты ДСКУ взаимодействуют с внешним миром через Агентов.



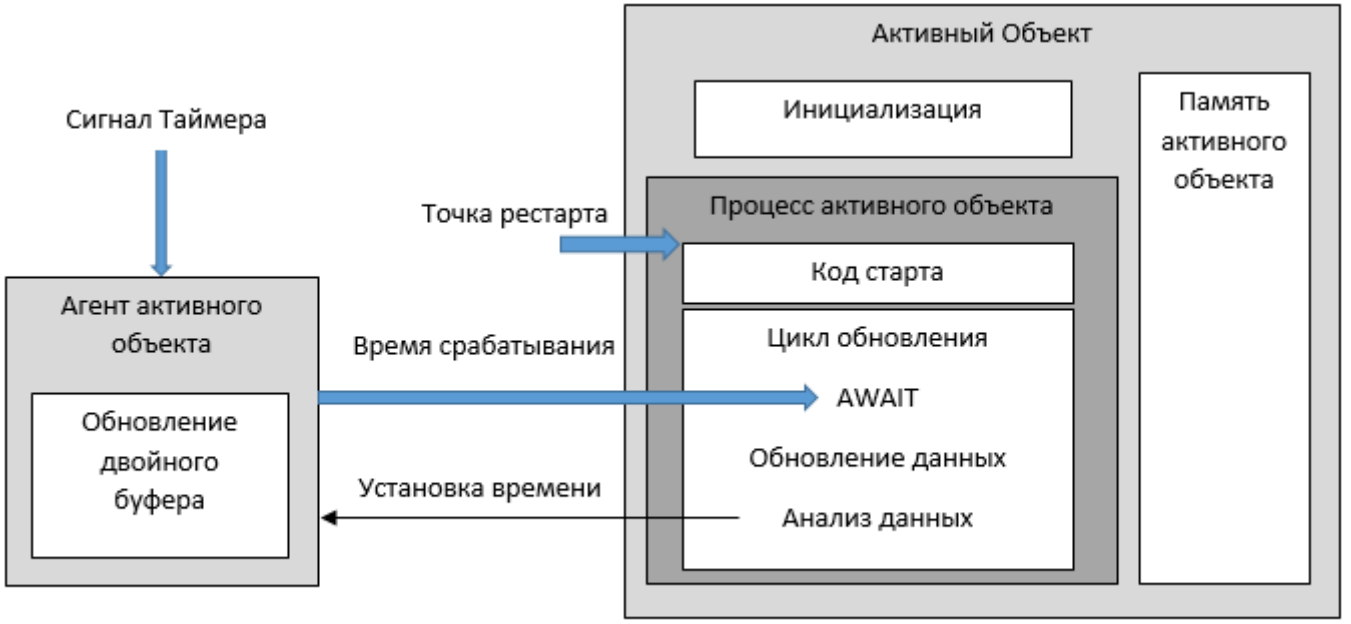
# Исключения активных объектов и механизм восстановления

Активные объекты содержат процессы внутри себя, система A2 обеспечивает инициализацию в главном процессе и выполнение тела {ACTIVE, SAFE} BODY активного объекта в контексте процесса активного объекта, начиная с Кода старта.

Память, выделенная при инициализации, постоянна и используется на протяжении всего времени жизни активного объекта.

При возникновении исключений при обновлении/анализе данных, тело активного объекта перехватывает трап и переходит к Точке рестарта.

Обработчик трапов обновляет массивы данных статистики.



# Гарантии отсутствия потерь при сетевых сбоях

1. Сетевая передача является надежной;
2. Латентность равна 0;
3. Пропускная способность бесконечна;
4. Транспортные издержки равны 0.

Циклическая передача всех данных фиксированного размера с циклом обновления 50 мс.

Даже при наличии многократных сетевых сбоев информация приходит в ДСКУ с некоторой задержкой, кратной периоду обмена.

# Отсутствуют переполнения времени и проблема 2038

1. Отсутствиуют переполнения времени;
2. Величина будущей временной метки всегда больше текущей;
3. Нет скрытых блокировок ожидания.

Проблема 2038, nanosleep для 32-битных и многих 64-битных ядер и системных библиотек Linux.

Единственный временной счетчик от начала работ – 64-битный TSP.

Отсутствие синхронизации времени.

Отсутствие привязки событий к ожидаемому времени в будущем.

# Презумпция неэргодичности

Программная система считается неэргодической, пока не доказано обратное.

Для представленной Оберон-системы приведены доказательства эргодичности в части:

- Управления памятью;
- Обеспечения реального времени;
- Механизма обработки исключений;
- Сетевого обмена данными;
- Обеспечения задатчика времени.

# #Второе седло для Боливара

Допущение о предоставлении требуемого сотрудничества в области системно-значимого ПО (ОС, компиляторы, …).

Отказ от диверсификации как принятие решения (отпустили запасную лощадь). При том, что Информатика-21 предлагает независимые диверсные (не альтернативные) экосистемы (Дом Оберона), выстроенные по видению Н.Вирта, Э.Дейсктры, Э.Хоара.

Ставка на единственные правильные технологии (C++, Win, Lin) и единственное правильное сотрудничество к организациями, являющимися стратегическими оппонентами РФ.

Вероятное неэргодичное состояние разрыва отношений (Боливар не выдержит двоих).

# Вопросы по докладу …

Дагаев Дмитрий Викторович,

Консультант проекта Информатика-21
forum.oberoncore.ru
www.inr.ac.ru/~info21/

dvdagaev@oberon.org

# Приложение 1. МЭК 62645 – Требования по защищенности программ СКУ

Разбиение на зоны безопасности, разделенные шлюзами.

Отсутствие **удаленного обновления** ПО (A, B);

Отсутствие **удаленной записи** данных: уставки, параметры БД (A);

Ограничение удаленной записи данных: уставки, параметры БД (B);