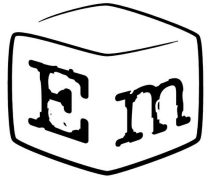


Повышение безопасности конечных систем с помощью специального языка описания модулей. Опыт Embox

Антон Бондарев

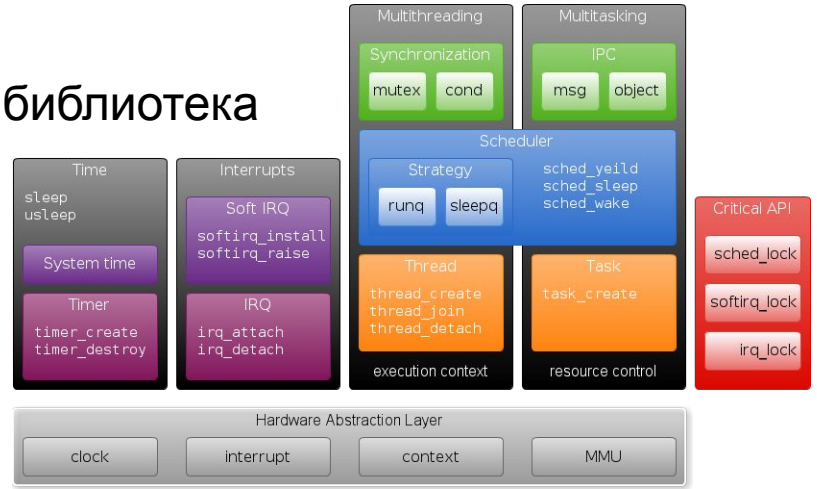
OS Day, 20 июня 2024

Embox

Embox — свободная операционная система реального времени (RTOS), разрабатываемая для встроенных систем.
Основная идея использование ПО **Линукс** в более безопасном и детерминированном, менее ресурсоемком и энергопотребляющем окружении

Embox

- Архитектуры ARM, x86, RISC-V, MIPS, SPARC, ...
- Полнофункциональная современная ОС
  - Ядро
    - Вытесняющая многозадачность
    - IPC
    - Управление памятью
    - …
  - Файловая система на VFS
  - Конфигурируемая стандартная библиотека
  - Собственный TCP/IP
  - Графическая подсистема
    - …



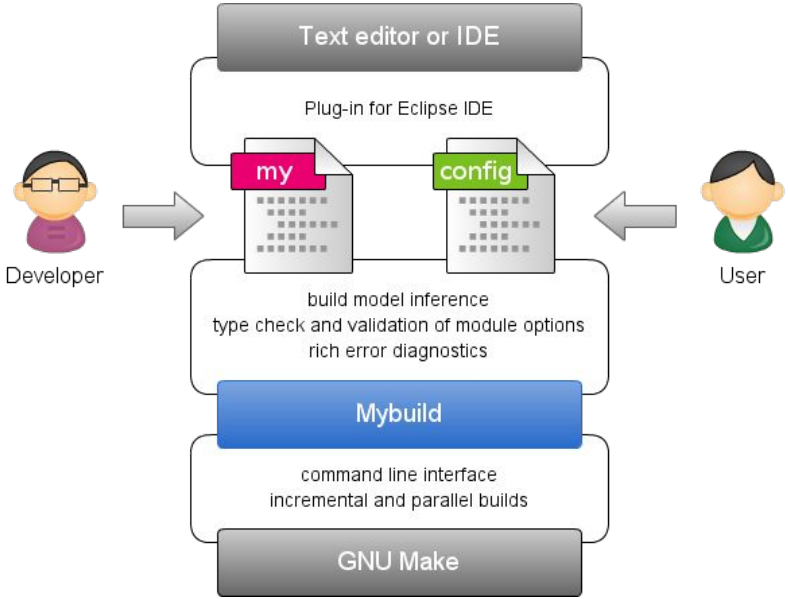
Embox

Операционная система под конкретную задачу, основанная на **специальном DSL языке** и использующая:

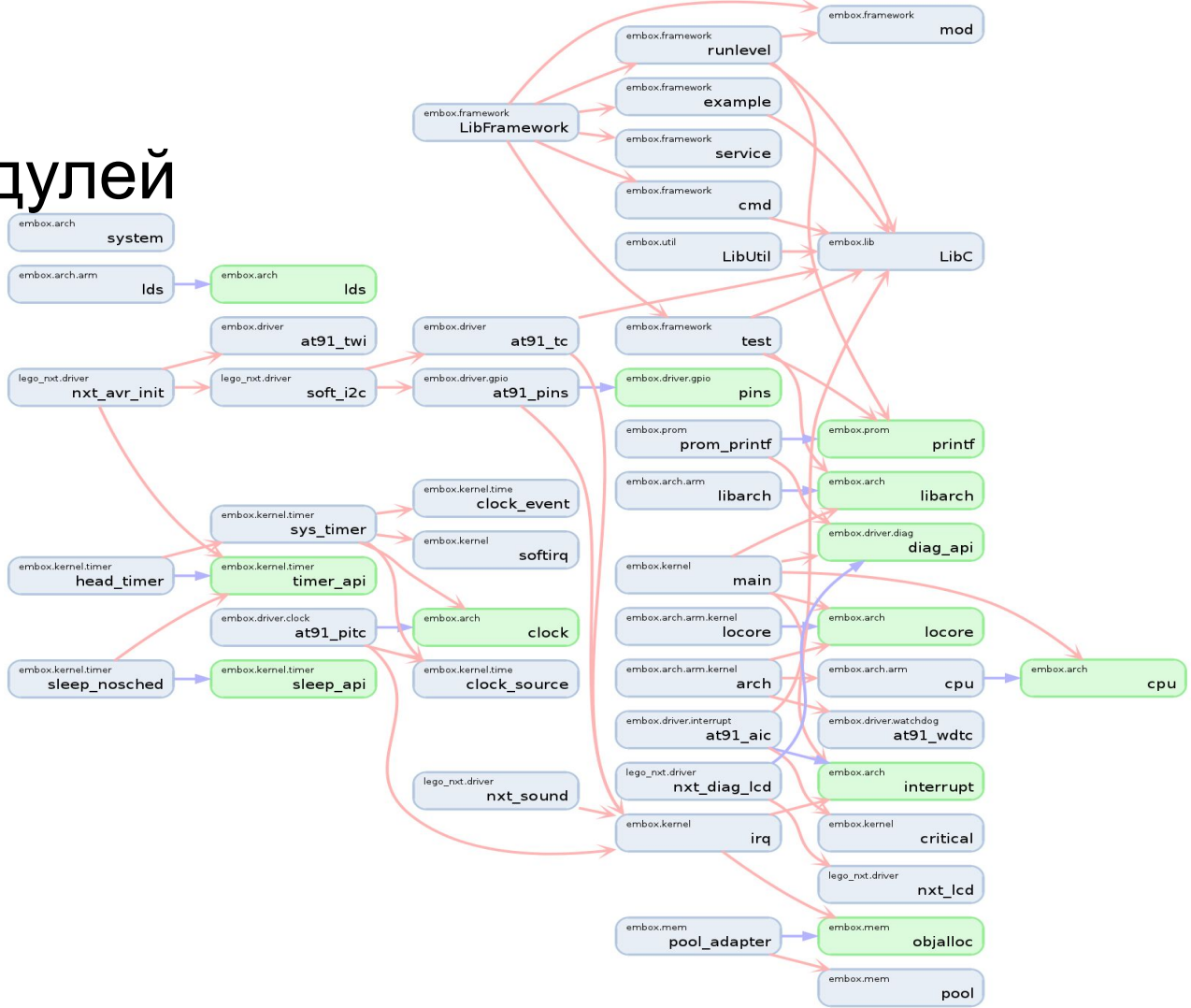
- Статическую информацию о задачах устройства
- Статическую конфигурацию системы
- Статический анализ зависимостей
- Статическую проверку параметров системы

Embox build system:
KBuild + OpenEmbedded + DevTree

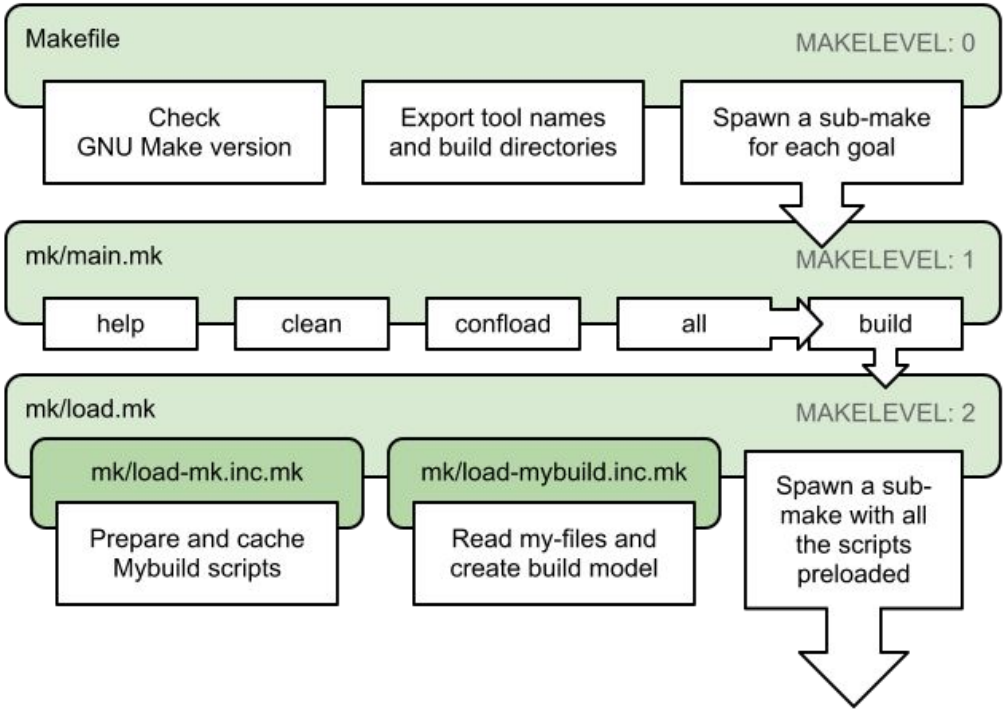
Embox. Процесс сборки



Граф модулей



Mybuild-процесс



Описание модулей

```
module irq extends irq_api {
    option number action_n = 0
    option number entry_n = 0

    source "irq.c"
    depends irq_lock
    @NoRuntime depends irq_stack
    @NoRuntime depends embox.mem.objalloc
    depends embox.driver.interrupt.irqctrl_api
    @NoRuntime depends embox.profiler.trace
}
```

Описание требований

```
configuration conf {
    @Runlevel(0) include embox.arch.x86.kernel.arch
    @Runlevel(0) include embox.arch.x86.kernel.locore
    @Runlevel(0) include embox.arch.x86.kernel.context
    @Runlevel(0) include embox.arch.x86.kernel.interrupt
    @Runlevel(0) include embox.arch.x86.mmu


    @Runlevel(1) include embox.driver.interrupt.i8259
    @Runlevel(1) include embox.driver.clock.pit
    @Runlevel(1) include embox.kernel.timer.sys_timer
    @Runlevel(1) include embox.kernel.time.kernel_time

    @Runlevel(1) include embox.kernel.timer.sleep
    @Runlevel(1) include embox.kernel.timer.strategy.list_timer
    @Runlevel(1) include embox.kernel.time.timekeeper
    @Runlevel(1) include embox.kernel.irq
    @Runlevel(1) include embox.kernel.critical
    @Runlevel(1) include embox.kernel.task.multi

    @Runlevel(1) include embox.kernel.timer.sleep
    @Runlevel(1) include embox.kernel.timer.strategy.list_timer
    @Runlevel(1) include embox.kernel.timer.sys_timer
    @Runlevel(1) include embox.kernel.time.kernel_time

    @Runlevel(2) include embox.driver.net.ne2k_pci
    @Runlevel(2) include embox.driver.net.loopback
    @Runlevel(2) include embox.driver.net.e1000
    @Runlevel(2) include embox.driver.virtual.null
    @Runlevel(2) include embox.driver.virtual.zero
    .
    .
    .
}
```

Статическое распределение памяти

/ region (origin, length) */*
ROM (0x08000000, 1M)
RAM (0x20000000, 512K)

/ section (region[, lma_region]) */*
text   (ROM)
rodata (ROM)
data   (RAM, ROM)
bss   (RAM)

section (flasher_text, RAM, ROM)
phdr (flasher_text, PT_LOAD, FLAGS(5))
section (flasher_rodata, RAM, ROM)
phdr (flasher_rodata, PT_LOAD, FLAGS(5))

Статическое распределение памяти

*include embox.mem.static_heap(**heap_size=0x4000**)*

*include embox.net.skbuff(**amount_skb=10**)*

*include embox.kernel.thread.core(**thread_pool_size=16, thread_stack_size=5000**)*

Статическое распределение памяти

./scripts/ld_map_info.sh build/base/obj/embox-2.o.map "\.bss"

Статическое распределение аппаратуры

```
[0] = {
        .status = ENABLED,
        .name = "UART0",
        .dev = {
                .name = "UART0",
                .regs = {
                        REGMAP("BASE_ADDR", (UART0_BASE), 0x100),
                },
                .irqs = {
                        VAL("", PLIC_UART0_VECTNUM),
                },
                .pins = {
                        PIN("TX", GPIO_PORT_A, 1, 1),
                        PIN("RX", GPIO_PORT_A, 0, 1),
                },
                .clocks = {
                        VAL("", "CLK_UART0"),
                }
        },
},
```

Статическое распределение аппаратуры

*include embox.driver.serial.stm_diag(baud_rate=115200, **usartx=1**)*

*@Runlevel(1) include embox.driver.serial.stm_ttyS0(baud_rate=115200, **usartx=1**)*

*@Runlevel(1) include embox.driver.serial.stm_ttyS1(baud_rate=115200, **usartx=6**)*

Статическое распределение аппаратуры

```
@Runlevel(0) include embox.arch.arm.cortexm3.armv7m_cpu_cache(
 log_level="LOG_DEBUG",
 sram_nocache_section_size=0x4000,
 nocache_region0_addr=0x60000000,
nocache_region0_size=0x00200000
```

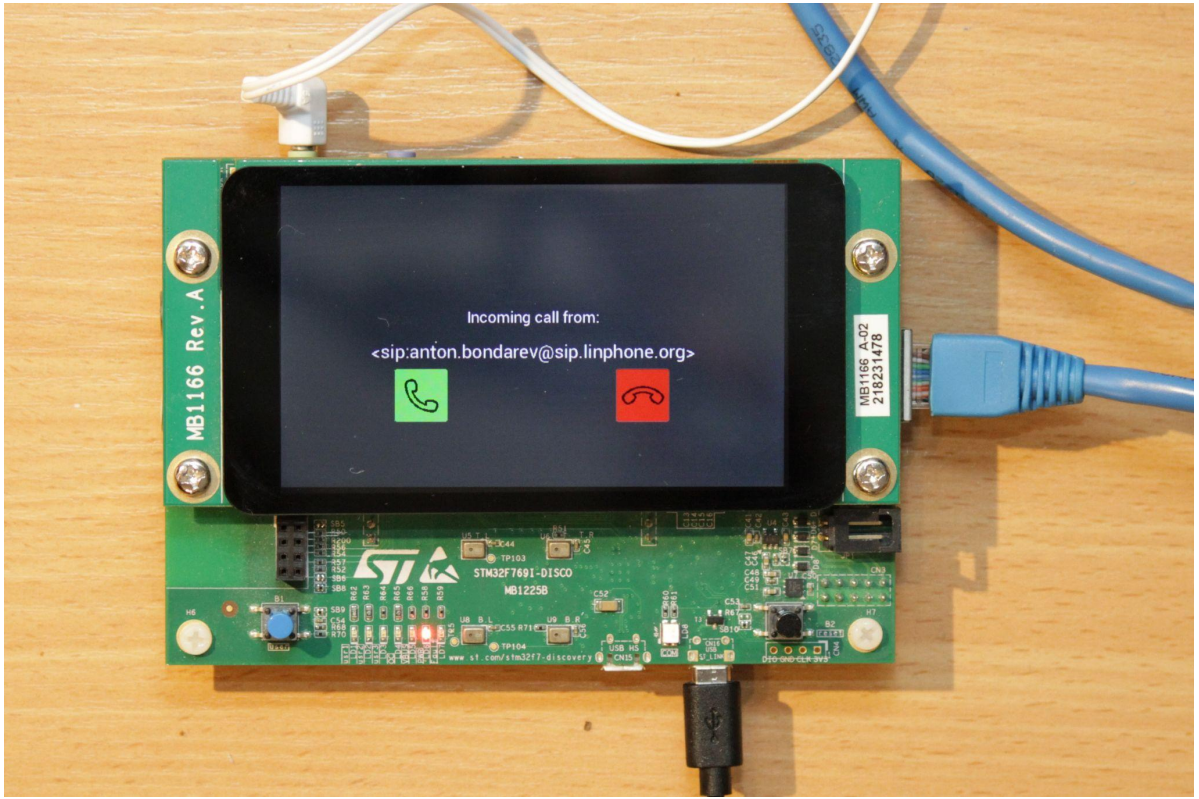
Embox: Hello world (Mybuild)

```
package embox.cmd


@AutoCmd
@Cmd(name = "hello_world", help="First Embox application")
module hello_world {
        source "hello_world.c"
}
```

Embox: Mybuild (BuildDepends)

```
@BuildDepends(gcc_build)

@BuildArtifactPath(cppflags_before="-I$(abspath
$(EXTERNAL_BUILD_DIR))/third_party/gcc/gcc_build/install/_target/include/c++/_gcc_version
-I$(abspath
$(EXTERNAL_BUILD_DIR))/third_party/gcc/gcc_build/install/_target/include/c++/_gcc_version/_target
")

static module libstdcxx extends embox.lib.libstdcxx {

    @AddPrefix("^BUILD/extbld/third_party/gcc/gcc_build/install/libs")

    source "libstdc++.a"

    @NoRuntime depends gcc_build

}
```

Embox: PJSIP

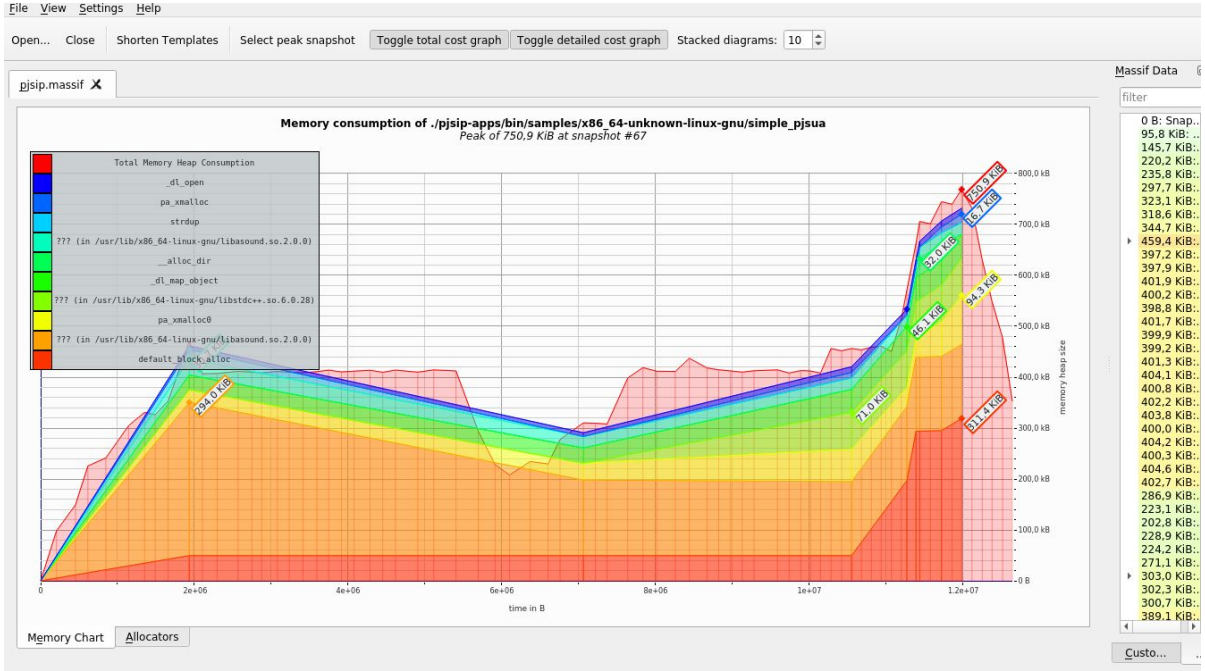

Incoming call from:
<sip:anton.bondarev@sip.linphone.org>
MB1166 Rev.A
STM32F769I-DISCO
MB1225B

PJSIP на Linux

```
$ ./configure \
        --prefix=$PREFIX \
        --disable-l16-codec   \
        --disable-ilbc-codec  \
        --disable-speex-codec \
        --disable-speex-aec   \
        --disable-gsm-codec   \
        --disable-g722-codec  \
        --disable-g7221-codec \
        --disable-libyuv \
        --disable-libwebrtc
$ make dep && make
```

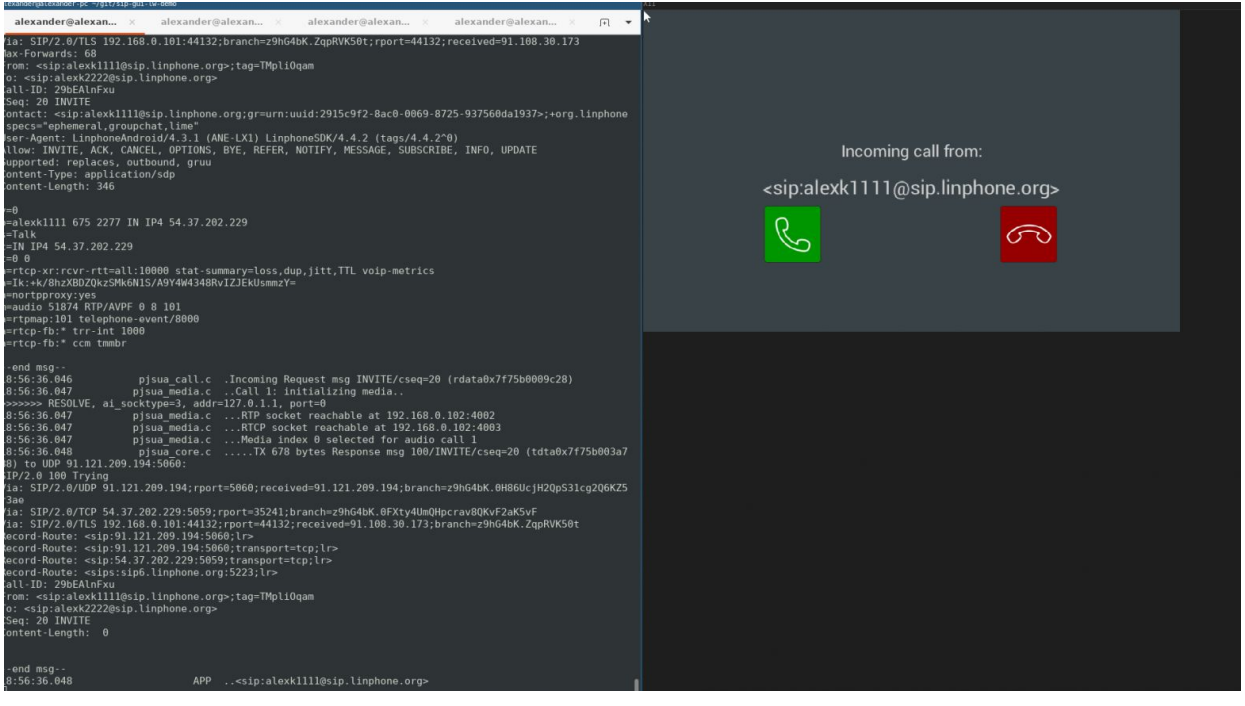
valgrind on Linux

- valgrind --tool=massif --time-unit=B --massif-out-file=pjsip.massif ./pjsip-apps/bin/samples/x86_64-unknown-linux-gnu/simple_pjsua
- massif-visualizer pjsip.massif



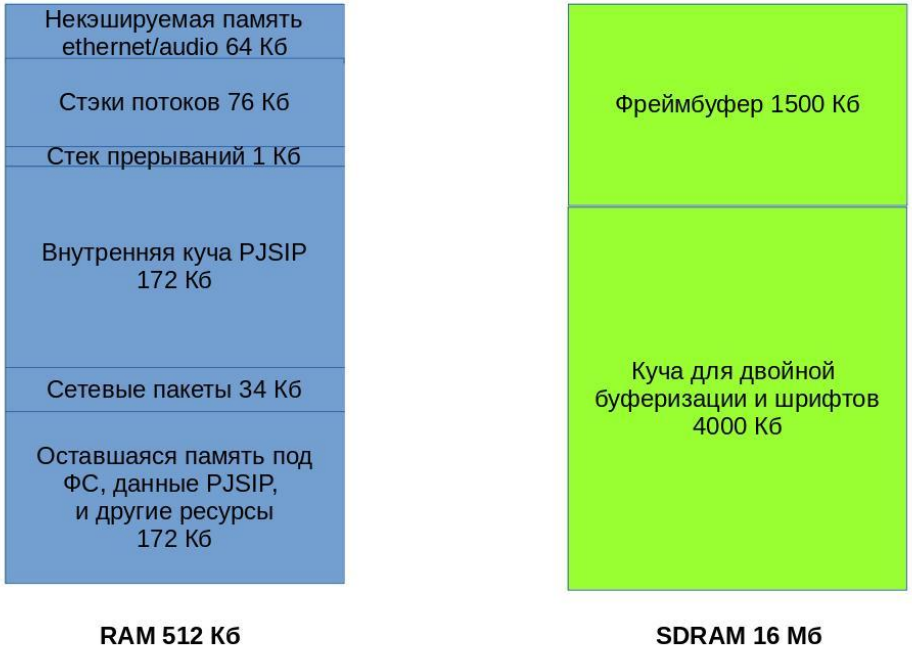
Embox: PJSIP on QEMU

- Добавили графический интерфейс
- Запустили на qemu

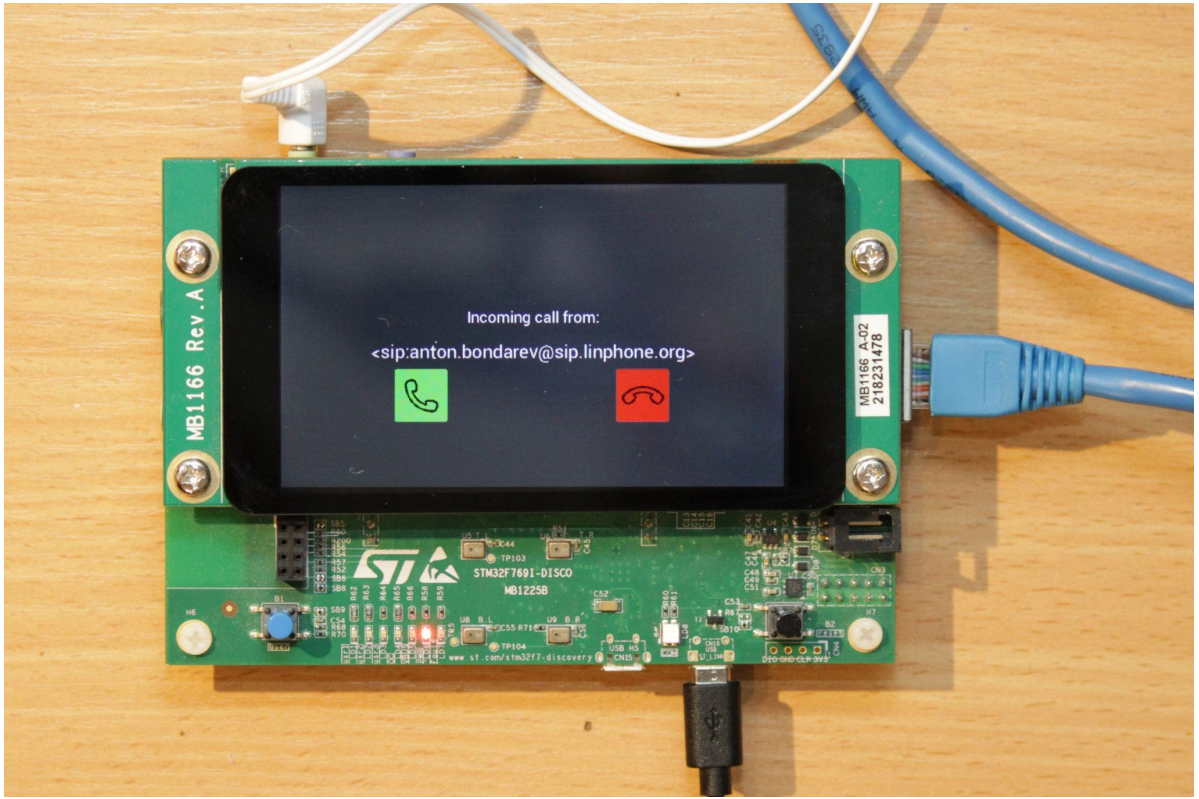


Embox: PJSIP на плате

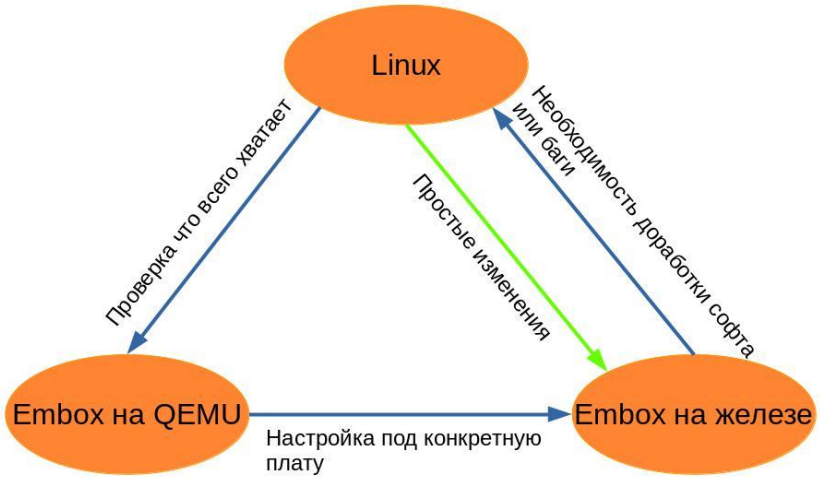
- карта памяти



Embox: PJSIP


Incoming call from:
<sip:anton.bondarev@sip.linphone.org>
MB1166 Rev.A
STM32F769I-DISCO
MB1225B

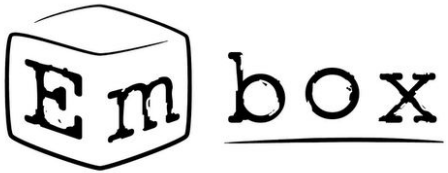
Процесс разработки под Embox



Заключение

- Проверки на этапе проектирования увеличивают безопасность конечных систем
- Необходимо внесение избыточности для описания требований и свойств
- Специализированный (DSL) язык хорошо подходит для описания требований
- Для увеличения безопасности необходимо внесение изменений в процесс разработки конечных систем

Contacts



Essential toolbox for embedded development

youtube

- **https://www.youtube.com/@embox-rtos**

Embox Project Homepage

- **http://embox.github.io/**

Telegram chat

- **https://t.me/embox_chat**