UNIVERSITY OF ZAGREB
**FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING**

MASTER THESIS num. 1981

# Software and Hardware Architecture for Redundant Embedded Systems

Dino Šarić

Zagreb, August 2020.

*Umjesto ove stranice umetnite izvornik Vašeg rada.*
*Kako biste uklonili ovu stranicu, obrišite naredbu* `\izvornik`.

*Thanks to my parents for supporting me financially and giving me an opportunity of studying away from home. Thanks to my aunt Dijana and my friends for supporting me emotionally. Thanks to all the helpful current and former students from the college forums. Finnally, thanks to the Youtubers that made understanding the college curriculum much easier.*

# Contents

**1. Functional safety in embedded systems** **1**

**2. Cortex R additions over cortex M** **2**

**3. FreeRTOS functional safety additions** **3**

3.1. Timed tasks . . . 3

3.1.1. Limitiations . . . 3

3.2. Replicated tasks . . . 3

3.2.1. Limitiations . . . 4

3.3. Commands reference . . . 4

3.3.1. xTaskCreateTimed - Creates a timed task. . . . 4

3.3.2. vTaskTimedReset - Resets the timer of timed task. . . . 8

3.3.3. xTimerGetTaskHandle - Gets the corresponding timed task handle from the timer handle. . . . 9

3.3.4. xTaskCreateReplicated - Creates a replicated task. . . . 9

3.3.5. xTaskSetCompareValue - Sets a compare value for the calling task. 13

3.3.6. vTaskSyncAndCompare - Syncronizes the replicated tasks and compares compare values. . . . 13

3.3.7. eTaskGetType - Get the type of the task. . . . 14

3.3.8. xTimerPause - Pauses the timer. . . . 14

3.3.9. xTimerPauseFromISR - Pauses the timer from interrupt service routine. . . . 15

3.3.10. xTimerResume - Resumes the timer. . . . 16

3.3.11. xTimerResumeFromISR - Resumes the timer from interrupt service routine. . . . 17

3.3.12. xTimerIsTimerActiveFromISR - Checks if timer is active from interrupt service routine. . . . 18

**4. Secure bootloader** **19**

4.1. What is a bootloader? . . . 19

4.2. Developed bootloader overview . . . . . 19
4.3. The bootloader's architecture . . . . . 20
4.4. Flash memory organization . . . . . 21
4.5. Application boot record . . . . . 22
4.6. User application modifications . . . . . 23
4.7. Command reference . . . . . 24
4.7.1. version - Gets a version of the bootloader. . . . . 24
4.7.2. help - Makes life easier. . . . . 25
4.7.3. reset - Resets the microcontroller. . . . . 25
4.7.4. cid - Gets chip identification number. . . . . 25
4.7.5. get-rdp-level - Gets read protection [3, p. 93] . . . . . 26
4.7.6. jump-to - Jumps to a requested address. . . . . 26
4.7.7. flash-erase - Erases flash memory. . . . . 26
4.7.8. flash-write - Writes to flash memory. . . . . 27
4.7.9. mem-read - Read bytes from memory. . . . . 28
4.7.10. update-act - Updates active application from new application memory area. . . . . 29
4.7.11. update-new - Updates new application. . . . . 29
4.7.12. en-write-prot - Enables write protection per sector. . . . . 31
4.7.13. dis-write-prot - Disables write protection per sector. . . . . 31
4.7.14. get-write-prot - Returns bit array of sector write protection. . . 32
4.7.15. exit - Exits the bootloader and starts the user application. . . . 32

**5. Conclusion** **33**

**Bibliography** **34**

# List of Figures

1. Texas refinery disaster . . . . . vii
2. Air France Concorde disaster . . . . . vii

4.1. Bootloader file structure for STM32F4007 microcontroller . . . . . 20
4.2. State machine of the bootloader . . . . . 21
4.3. Example of an error from error state . . . . . 21

# Introduction

In a world with increasing number of electronic systems in hazardous environment, the correct operation of active systems is ever more important for ensuring less catastrophes. In year 2000, Air France Concorde flight crashed soon after its take-of killing 113 people, in 2005 Texas City refinery exploded killing 15 people and injuring 180. Similar disasters to these were the motivation for the creation of functional safety principles.

**Figure 1:** Texas refinery disaster

**Figure 2:** Air France Concorde disaster

Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.[2] In other words, the goal of functional safety is ensuring even when the system fails its response is predictable and safe. Today, the concept of functional safety is part of everyday life and applies to every industry one can think of. For example, functional safety ensures that airbags in a car instantly deploy during impact to protect the passengers. Another good example is an automated flight control system in the airplanes. Autopilot controls pitch and roll of the aircraft changing the heading and altitude, all of which is developed with respect to functional safety parameters, activating alarms and other measures when they are breached.[2]

Motivation of this paper is exploring how are principles of functional safety applied to the engineering projects. Investigate how and why redundancy is implemented in hardware and software. As a part of that, redundant microcontrollers are explored and compared to non-redundant counterparts. Additionally, functional safety additions to FreeRTOS operating system are implemented. Modifications add task replication and a option to measure execution time of tasks. Finally, secure bootloader is added,

bootloader has a command shell interface and has option of updating the current application.

The thesis is organized in the following way. Chapter 1 gives brief introduction of functional safety process. Moreover, chapter gives a overview of how is hardware of embedded systems designed to support redundancy. Chapter 2 investigates ARM Cortex R microcontroller inner workings and what do they add over Cortex M. Chapter 3 gives overview of added safety functions to the FreeRTOS kernel and gives a brief overview of FreeRTOS's inner workings. Chapter 4 explains how the developed secure bootloader functions and its features.

# 1. Functional safety in embedded systems

Opis functional safety-a, definicija, proces... **TODO**

HW **TODO**

SW **TODO**

# 2. Cortex R additions over cortex M

**TODO** uniti koje imaju pojedine cortex r implementacije **TODO** Sto cortex M ima

# 3. FreeRTOS functional safety additions

**TODO** Opis FreeRTOS-a.

**TODO** Dodati strukturu foldera.

## 3.1. Timed tasks

**TODO: Opis kako funcionira.**

**TODO** Motivacija za timed tasks, periodicki taskovi Jeleknovic.

Timed tasks have an ability to track their own execution time. On initialization, time limit is set. If time limit is overreached error callback is called. Timed tasks make use of FreeRTOS timers.

### 3.1.1. Limitiations

Static create of the function is not available.

Timer callback functions are called by the timer daemon and its priority determines when the callback will be called. It is recommended that timer deamon has the highest priority.

## 3.2. Replicated tasks

**TODO: Motivacija, zasto 1oo2D i 2oo3D.**

**TODO: Opis kako funcionira.**

Replicated tasks have an ability to detect errors using at least two tasks performing identical operations. Tasks are independently processed by the processor. Output variables from tasks are compared in real time. In case of discrepancy in the output variables, an error callback is called where user can process the error.

### 3.2.1. Limitiations

Static create of the function is not available.

Timer callback functions are called by the timer daemon and its priority determines when the callback will be called. It is recommended that timer deamon has the highest priority.

## 3.3. Commands reference

Timed tasks:

- xTaskCreateTimed - Creates a timed task
- vTaskTimedReset - Resets the timer of timed task
- xTimerGetTaskHandle - Gets the corresponding timed task handle from the timer handle

Replicated tasks:

- xTaskCreateReplicated - Creates a replicated task
- xTaskSetCompareValue - Sets a compare value for the calling task
- vTaskSyncAndCompare - Syncronizes the replicated tasks and compares compare values

General added functions:

- eTaskGetType - Get the type of the task
- xTimerPause - Pauses the timer
- xTimerPauseFromISR - Pauses the timer from interrupt service routine
- xTimerResume - Resumes the timer
- xTimerResumeFromISR - Resumes the timer from interrupt service routine
- xTimerIsTimerActiveFromISR - Checks if timer is active from interrupt service routine

### 3.3.1. xTaskCreateTimed - Creates a timed task.

```
1 BaseType_t xTaskCreateTimed( TaskFunction_t pxTaskCode,
2                     const char * const pcName,
3                     const configSTACK_DEPTH_TYPE usStackDepth,
4                     void * const pvParameters,
5                     UBaseType_t uxPriority,
```

```
6                       TaskHandle_t * const pxCreatedTask,
7                       TickType_t xOverrunTime,
8                       WorstTimeTimerCb_t pxOverrunTimerCb,
9                       TickType_t xOverflowTime,
10                      WorstTimeTimerCb_t pxOverflowTimerCb )
```

Create a new timed task and add it to the list of tasks that are ready to run.

Overrun timer is synchronous with the task and its counter is incremented only when timed task is in running state. Overrun callback is called from timer daemon. When timed task overruns it sends a signal to the timer daemon and when callback is called is dependent on daemon's priority. If overrun timer is not used send 0 for xOverrunTime or NULL for the callback.

Overflow timer is asynchronous with the task and its counter is incremented every tick regardless of the state. Callback is called from timer daemon and its punctuality is dependent on timer daemon's priority. If overflow timer is not used send 0 for xOverflowTime or NULL for the callback.

Internally, within the FreeRTOS implementation, tasks use two blocks of memory. The first block is used to hold the task's data structures. The second block is used by the task as its stack. If a task is created using xTaskCreateTimed() then both blocks of memory are automatically dynamically allocated inside the xTaskCreate() function. (see http://www.freertos.org/a00111.html). Static version of the function is not implemented.

Input paramters:
 - pvTaskCode - Pointer to the task entry function. Tasks
must be implemented to never return (i.e. continuous loop).

- pcName - A descriptive name for the task. This is mainly used to facilitate debugging. Max length defined by configMAX_TASK_NAME_LEN - default is 16.

- usStackDepth -The size of the task stack specified as the number of variables the stack can hold - not the number of bytes. For example, if the stack is 16 bits wide and usStackDepth is defined as 100, 200 bytes will be allocated for stack storage.

- pvParameters - Pointer that will be used as the parameter for the task being created.

- uxPriority - The priority at which the task should run. Systems that include MPU support can optionally create tasks in a privileged (system) mode by setting bit portPRIVILEGE_BIT of the priority parameter. For example, to create a privileged task at priority 2 the uxPriority parameter should be set to ( 2 | portPRIVILEGE_BIT ).

- pvCreatedTask - Used to pass back a handle by which the created task can be referenced.

- xOverrunTime - Runtime of the task after which callback will be called.

- pxOverrunTimerCb - Pointer to the function that will be called if task runs longer than xOverrunTime without reseting the timed task. Overrun timer is synchronous with the task and its tick is only incremented when timed task is in running state.

- xOverflowTime - Asynchronous timer time. After xOverflowTime pxOverflowTimerCb will be called.

- pxOverflowTimerCb - Pointer to the function that will be called after xOverflowTime. Overflow timer is asynchronous from the task and its value is incremented every tick.

Returns pdPASS if the task was successfully created and added to a ready list, otherwise an error code defined in the file projdefs.h
Example usage:

```
1  // Task to be created.
2  void vTaskTimedCode( void * pvParameters )
3  {
4      for( ;; )
5      {
6          // Task code goes here.
7
8          // Reset the timer.
```

```
9           vTaskTimedReset(NULL);
10      }
11  }
12
13  // Function to be called if timer overflows.
14  void vTaskOverflowCallback ( WorstTimeTimerHandle_t xTimer )
15  {
16      // Timeout callback code.
17
18      // Maybe task deletion is needed. Calling vTaskDelete
        ↪ automatically deletes
19      // the timer too. Do NOT delete the timer directly. That will
        ↪ cause
20      // undefined behavior when deleting the task.
21      vTaskDelete( xTimerGetTaskHandle( xTimer ) );
22  }
23  // Function to be called if timer overflows.
24  void vTaskOverrunCallback ( WorstTimeTimerHandle_t xTimer )
25  {
26
27      // Timeout callback code.
28
29      // Maybe task deletion is needed. Calling vTaskDelete
        ↪ automatically deletes
30      // the timer too. Do NOT delete the timer directly. That will
        ↪ cause
31      // undefined behavior when deleting the task.
32      vTaskDelete( xTimerGetTaskHandle( xTimer ) );
33  }
34
35   // Function that creates a task.
36   void vOtherFunction( void )
37   {
38   static uint8_t ucParameterToPass;
39   TaskHandle_t xHandle = NULL;
40
```

```
41      // Create the task, storing the handle.  Note that the passed
        ↪  parameter ucParameterToPass
42      // must exist for the lifetime of the task, so in this case is
        ↪  declared static.  If it was just an
43      // an automatic stack variable it might no longer exist, or at
        ↪  least have been corrupted, by the time
44      // the new task attempts to access it.
45      xTaskCreate( vTaskCode,
46                   "NAME",
47                   STACK_SIZE,
48                   &ucParameterToPass,
49                   tskIDLE_PRIORITY,
50                   &xHandle,
51                   pdMS_TO_TICKS(1 * 1000),
52                   vTaskOverrunCallback,
53                   pdMS_TO_TICKS(2 * 1000),
54                   vTaskOverflowCallback );
55      configASSERT( xHandle );
56
57      // Use the handle to delete the task.
58      if( xHandle != NULL )
59      {
60          vTaskDelete( xHandle );
61      }
62  }
```

### 3.3.2. vTaskTimedReset - Resets the timer of timed task.

```
1  void vTaskTimedReset( TaskHandle_t pxTaskHandle )
```

Reset the timer of the timed task.

- Warning - Shall only be used for timed tasks.

Input parameters:

- pxTaskHandle - Handle of the task whose timer shall be reset.
Passing a NULL handle results in reseting the timer of the calling task.

Example usage:

```
void vTimedTask( void * pvParameters )
{
    for( ;; )
    {
        // Task code goes here.

        vTaskTimedReset(NULL);
    }
}
```

### 3.3.3. xTimerGetTaskHandle - Gets the corresponding timed task handle from the timer handle.

```
TaskHandle_t xTimerGetTaskHandle( const TimerHandle_t xTimer )
```

Returns the timed task handle assigned to the timer. Task handle is an union with timer ID and that is why they are mutually exclusive.

Task handle is assigned to the timer when creating the timed task.

WARNING: Setting the timer ID also sets the task handle. Changing the timer ID can lead to undefined behavior.

Input parameters:

- xTimer - The timer being queried.

Example usage:

- See xTaskCreateTimed

### 3.3.4. xTaskCreateReplicated - Creates a replicated task.

```
BaseType_t xTaskCreateReplicated( TaskFunction_t pxTaskCode,
                                  const char * const pcName,
```

```
3                                   const configSTACK_DEPTH_TYPE
                                    ↪  usStackDepth,
4                                   void * const pvParameters,
5                                   UBaseType_t uxPriority,
6                                   TaskHandle_t * const pxCreatedTask,
7                                   uint8_t ucReplicatedType,
8                                   RedundantValueErrorCb_t
                                    ↪  pxRedundantValueErrorCb )
```

Create a new replicated task and add it to the list of tasks that are ready to run. Replicated task is used to achieve redundancy of the software at the expense of slower execution. Task executes slower because it is replicated two or three times. Depending on the type chosen. On every call to vTaskSyncAndCompare task is suspended until every replicated task arrives to the same point. When every task is in the synchronization function comparison is done. If any of the comparison results differ callback function pxRedundantValueErrorCb is called. In the callback function user can access the compare values and choose whether to delete all the tasks.

Internally, within the FreeRTOS implementation, tasks use two blocks of memory. The first block is used to hold the task's data structures. The second block is used by the task as its stack. If a task is created using xTaskCreateReplicated() then both blocks of memory are automatically dynamically allocated inside the xTaskCreateReplicated() function. (see http://www.freertos.org/a00111.html). Static version of this function is not implemented.

Input parameters:
- pvTaskCode - Pointer to the task entry function. Tasks
must be implemented to never return (i.e. continuous loop).

- pcName - A descriptive name for the task. This is mainly used to
 facilitate debugging. Max length defined by configMAX_TASK_NAME_LEN -
    default
 is 16.

- usStackDepth - The size of the task stack specified as the number of
variables the stack can hold - not the number of bytes. For example, if

the stack is 16 bits wide and usStackDepth is defined as 100, 200 bytes will be allocated for stack storage.

- pvParameters - Pointer that will be used as the parameter for the task being created.

- uxPriority - The priority at which the task should run. Systems that include MPU support can optionally create tasks in a privileged (system) mode by setting bit portPRIVILEGE_BIT of the priority parameter. For example, to create a privileged task at priority 2 the uxPriority parameter should be set to ( 2 | portPRIVILEGE_BIT ).

- pvCreatedTask - Used to pass back a handle by which the created task can be referenced.

- ucReplicatedType - Valid values: taskREPLICATED_NO_RECOVERY and taskREPLICATED_RECOVERY. No recovery is faster as it created only two instances, but recovery is not possible. Recovery creates three identical tasks. Recovery is possible with 2 out of 3 logic.

- pxRedundantValueErrorCb - Function to be called when compare values do not match. Return value determines whether calling redundant task will be deleted.

Returns pdPASS if the task was successfully created and added to a ready list, otherwise an error code defined in the file projdefs.h

Example usage:

```
1  // Task to be created.
2  void vTaskCode( void * pvParameters )
3  {
4      for( ;; )
5      {
6          // Task code goes here.
7
8          vTaskSyncAndCompare(&xCompareValue);
9      }
```

```
10  }
11
12  // NOTE: This function is called from the redundant task and not
    ↪  daemon.
13  uint8_t ucCompareErrorCb (CompareValue_t * pxCompareValues, uint8_t
    ↪  ucLen)
14  {
15      // Iterate through compare values.
16      for(uint8_t iii = 0; iii < ucLen; i++)
17      {
18          pxCompareValue[iii]
19          .
20          .
21          .
22      }
23
24      return pdTRUE; // Signaling to delete the redundant task.
25  }
26
27  // Function that creates a task.
28  void vOtherFunction( void )
29  {
30  static uint8_t ucParameterToPass;
31  TaskHandle_t xHandle = NULL;
32
33      // Create the task, storing the handle.  Note that the passed
        ↪  parameter ucParameterToPass
34      // must exist for the lifetime of the task, so in this case is
        ↪  declared static.  If it was just an
35      // an automatic stack variable it might no longer exist, or at
        ↪  least have been corrupted, by the time
36      // the new task attempts to access it.
37      xTaskCreateReplicated( vTaskCode, "NAME", STACK_SIZE,
        ↪  &ucParameterToPass, tskIDLE_PRIORITY, &xHandle,
        ↪  taskREPLICATED_RECOVERY, ucCompareErrorCb );
38      configASSERT( xHandle );
39
```

```
40      // Use the handle to delete the task.
41      if( xHandle != NULL )
42      {
43          vTaskDelete( xHandle );
44      }
45  }
```

### 3.3.5. xTaskSetCompareValue - Sets a compare value for the calling task.

```
1  void xTaskSetCompareValue( CompareValue_t xNewCompareValue )
```

Sets the compare value. Compare value is used with replicated tasks. They are used in vTaskSyncAndCompare function for figuring if there is a difference between the tied task executions.
Input parameters:
- xNewCompareValue - New compare value to set.

### 3.3.6. vTaskSyncAndCompare - Syncronizes the replicated tasks and compares compare values.

```
1  void vTaskSyncAndCompare( const CompareValue_t * const
   ↪  pxNewCompareValue )
```

Waits until every replicated task is finished. When every task is finished function compares the compare values and if there is a mismatch it calls the predefined callback.

- Warning - Shall only be used for replicated tasks.

Input parameters:

- pxNewCompareValue - Pointer of the compare value to be copied from. If NULL is passed in, previous compare value is used.

Example usage:

```
1  void vReplicatedTask( void * pvParameters )
2  {
```

```
    for( ;; )
    {
        // Task code goes here.

        vTaskSyncAndCompare(&xCompareValue);
    }
}
```

### 3.3.7. eTaskGetType - Get the type of the task.

```
eTaskType eTaskGetType( TaskHandle_t pxTaskHandle )
```

Get the type of the task.

Input parameters:

- pxTaskHandle - Handle of the task to be queried. Passing a NULL handle results in getting the type of calling task.

### 3.3.8. xTimerPause - Pauses the timer.

```
BaseType_t xTimerPause( TimerHandle_t xTimer, TickType_t xTicksToWait )
```

Timer functionality is provided by a timer service/daemon task. Many of the public FreeRTOS timer API functions send commands to the timer service task through a queue called the timer command queue. The timer command queue is private to the kernel itself and is not directly accessible to application code. The length of the timer command queue is set by the configTIMER_QUEUE_LENGTH configuration constant.

xTimerPause() pauses a timer. If timer was not running before it is ignored. Pausing remembers how many ticks until the deadline are needed and on next xTimerResume() timer will trigger only after the ticks set by pause.

Pausing assures timer is in stopped state.

- xTimer - The handle of the timer being paused.

- TicksToWait - Specifies the time, in ticks, that the calling task should

be held in the Blocked state to wait for the stop command to be successfully sent to the timer command queue, should the queue already be full when xTimerPause() was called. xTicksToWait is ignored if xTimerPause() is called before the scheduler is started.

Returns pdFAIL if the pause command could not be sent to timer command queue even after xTicksToWait ticks had passed. pdPASS will be returned if the command was successfully sent to the timer command queue.
When the command is actually processed will depend on the priority of the timer service/daemon task relative to other tasks in the system. The timer service/daemon task priority is set by the configTIMER_TASK_PRIORITY configuration constant.

### 3.3.9. xTimerPauseFromISR - Pauses the timer from interrupt service routine.

```
1 BaseType_t xTimerPauseFromISR( TimerHandle_t xTimer,
2                                BaseType_t *pxHigherPriorityTaskWoken
                                 ↪  );
```

A version of xTimerPause() that can be called from an interrupt service routine.

- xTimer - The handle of the timer being paused.

- pxHigherPriorityTaskWoken - The timer service/daemon task spends most of its time in the Blocked state, waiting for messages to arrive on the timer command queue. Calling xTimerPauseFromISR() writes a message to the timer command queue, so has the potential to transition the timer service/daemon task out of the Blocked state. If calling xTimerPauseFromISR() causes the timer service/daemon task to leave the Blocked state, and the timer service/ daemon task has a priority equal to or greater than the currently executing task (the task that was interrupted), then *pxHigherPriorityTaskWoken will get set to pdTRUE internally within the xTimerPauseFromISR() function. If xTimerPauseFromISR() sets this value to pdTRUE then a context switch should be performed before the interrupt exits.

Returns pdFAIL if the pause command could not be sent to the timer command queue. pdPASS will be returned if the command was successfully sent to the timer command queue. When the command is actually processed will depend on the priority of the timer service/daemon task relative to other tasks in the system. The timer service/daemon task priority is set by the configTIMER_TASK_PRIORITY configuration constant.

### 3.3.10. xTimerResume - Resumes the timer.

```
1 BaseType_t xTimerResume( TimerHandle_t xTimer, TickType_t xTicksToWait
  ↪ )
```

Timer functionality is provided by a timer service/daemon task. Many of the public FreeRTOS timer API functions send commands to the timer service task through a queue called the timer command queue. The timer command queue is private to the kernel itself and is not directly accessible to application code. The length of the timer command queue is set by the configTIMER_QUEUE_LENGTH configuration constant.

xTimerResume() resumes a timer. If timer was not running before it acts as xTimerStart. If timer saw stopped prior to the call with xTimerPause than it places a deadline in daemon task from the time timer left of and not the full period.

Resuming assures timer is in running state. If the timer is not stopped, deleted, or reset in the mean time, the callback function associated with the
timer will get called 'n' ticks after xTimerStart() was called, where 'n' is the time left from when last pause was called.

- xTimer - The handle of the timer being resumed.

- xTicksToWait - Specifies the time, in ticks, that the calling task should be held in the Blocked state to wait for the resume command to be successfully sent to the timer command queue, should the queue already be full when xTimerResume() was called. xTicksToWait is ignored if xTimerResume() is called before the scheduler is started.

pdFAIL will be returned if the resume command could not be sent to the timer command queue even after xTicksToWait ticks had passed. pdPASS

will be returned if the command was successfully sent to the timer command queue. When the command is actually processed will depend on the priority of the timer service/daemon task relative to other tasks in the system. The timer service/daemon task priority is set by the configTIMER_TASK_PRIORITY configuration constant.

### 3.3.11. xTimerResumeFromISR - Resumes the timer from interrupt service routine.

```
1 BaseType_t xTimerResumeFromISR( TimerHandle_t xTimer,
2                                 BaseType_t *pxHigherPriorityTaskWoken
                                  ↪ )
```

A version of xTimerResume() that can be called from an interrupt service routine.

- xTimer - The handle of the timer being resumed.

- pxHigherPriorityTaskWoken - The timer service/daemon task spends most of its time in the Blocked state, waiting for messages to arrive on the timer command queue. Calling xTimerPauseFromISR() writes a message to the timer command queue, so has the potential to transition the timer service/daemon task out of the Blocked state. If calling xTimerPauseFromISR() causes the timer service/daemon task to leave the Blocked state, and the timer service/ daemon task has a priority equal to or greater than the currently executing task (the task that was interrupted), then *pxHigherPriorityTaskWoken will get set to pdTRUE internally within the xTimerPauseFromISR() function. If xTimerPauseFromISR() sets this value to pdTRUE then a context switch should be performed before the interrupt exits.

pdFAIL will be returned if the resume command could not be sent to the timer command queue. pdPASS will be returned if the command was successfully sent to the timer command queue. When the command is actually processed will depend on the priority of the timer service/daemon task relative to other tasks in the system. The timer service/daemon task priority is set by the configTIMER_TASK_PRIORITY configuration constant.

### 3.3.12. xTimerIsTimerActiveFromISR - Checks if timer is active from interrupt service routine.

```
1 BaseType_t xTimerIsTimerActiveFromISR( TimerHandle_t xTimer );

A version of xTimerIsTimerActive() that can be called from an interrupt
    service
routine.

- xTimer - The handle of the timer that is to be checked.

pdFAIL will be returned if the reset command could not be sent to
the timer command queue. pdPASS will be returned if the command was
successfully sent to the timer command queue. When the command is actually
processed will depend on the priority of the timer service/daemon task
relative to other tasks in the system, although the timers expiry time is
relative to when xTimerResetFromISR() is actually called. The timer service/
    daemon
task priority is set by the configTIMER_TASK_PRIORITY configuration constant
    .
```

# 4. Secure bootloader

## 4.1. What is a bootloader?

Bootloaders are usually the first pieces of code that run, they run just before the user's application e.g. an operating system. They are used to manage the memory. It is highly processor and board specific. The term "bootloader" is a shortened form of the words "bootstrap loader". The term stems from the fact that the boot manager is the key component in starting up the computer, so it can be likened to the support of a bootstrap when putting a boot on.[1]

## 4.2. Developed bootloader overview

Developed bootloader can be controlled using a command shell communication over UART. The bootloader has an ablility to load new application over UART. In addition, a number of memory management functions are added. When updating the application bootloader accepts three types: binary (.bin), Intel hex (.hex) or Morotola S-record (.srec). Transmitted new application can additionally be checksummed with SHA256 or cyclic redundancy check (CRC32).

The default STM32F407 microcontroller's bootloader doesn't allow the aforementioned functionality and that is the main motivation for writing code for this platform. [3] First version of the bootloader is developed for STM32F407-Discovery board. Bootloader code is situated in the first three sectors of microcontrollers memory, as seen in Table 4.1. Fourth section is used as persistent memory (not loaded on the code startup) for communication between bootloader and user's application. More about application boot record in section 4.5.

Bootlader is written according to the BARR:C-2018 C coding standard to minimize defects in code. [4]

File structure of the bootloader source code for STM32F407 is as follows:

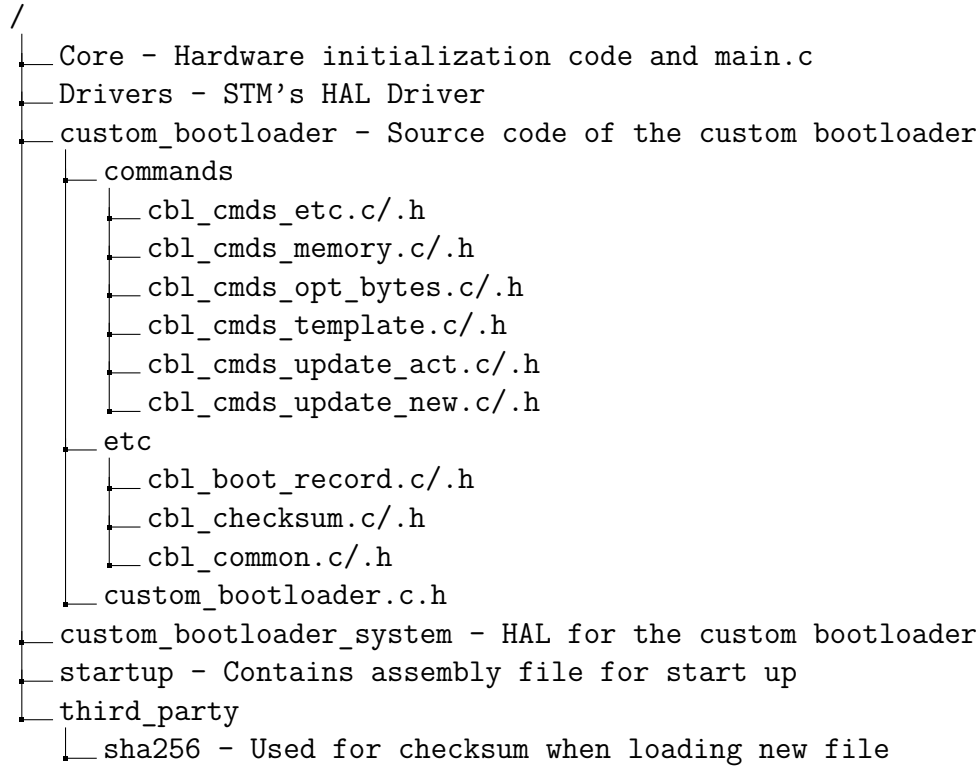


**Figure 4.1:** Bootloader file structure for STM32F4007 microcontroller

## 4.3. The bootloader's architecture

The bootloader architecture is simple. On entry, the bootloader checks if blue button on the discovery board is pressed, if it is pressed bootloader is skipped and user's application starts. Bootloader starts otherwise. On bootloader start, it checks if user's application update is needed and updates it if needed. Next step is going into system state machine.

Bootloader has 3 states: Operation, error and exit. Operation state flow is shown in Figure 4.2. Operation state waits for incomming commands and processes them, error state constructs and sends error message back to the user. Exit state is called right before exiting, it is used to deconstruct data from the bootloader.

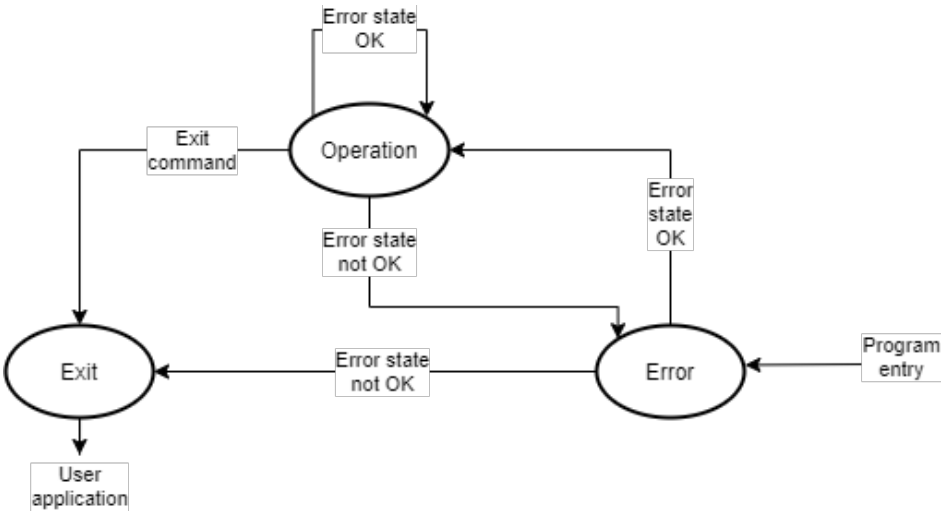


**Figure 4.2:** State machine of the bootloader

```
> get-write-pro

ERROR: Invalid command

>
```

**Figure 4.3:** Example of an error from error state

## 4.4. Flash memory organization

When using the bootloader the flash module is organized a shown in Table 4.1.

| Block | Used by | Name | Block base addresses | Size |
|---|---|---|---|---|
| Main memory | Bootloader | Sector 0 | 0x0800 0000 - 0x0800 3FFF | 16 Kbytes |
| | | Sector 1 | 0x0800 4000 - 0x0800 7FFF | 16 Kbytes |
| | | Sector 2 | 0x0800 8000 - 0x0800 BFFF | 16 Kbytes |
| | Boot record | Sector 3 | 0x0800 C000 - 0x0800 FFFF | 16 Kbytes |
| | Current application | Sector 4 | 0x0801 0000 - 0x0801 FFFF | 64 Kbytes |
| | | Sector 5 | 0x0802 0000 - 0x0803 FFFF | 128 Kbytes |
| | | Sector 6 | 0x0804 0000 - 0x0805 FFFF | 128 Kbytes |
| | | Sector 7 | 0x0806 0000 - 0x0807 FFFF | 128 Kbytes |
| | New application | Sector 8 | 0x0808 0000 - 0x0809 FFFF | 128 Kbytes |
| | | Sector 9 | 0x080A 0000 - 0x080B FFFF | 128 Kbytes |
| | | Sector 10 | 0x080C 0000 - 0x080D FFFF | 128 Kbytes |
| | | Sector 11 | 0x080E 0000 - 0x080F FFFF | 128 Kbytes |
| System memory | | | 0x1FFF 0000 - 0x1FFF 77FF | 30 Kbytes |
| OTP area | | | 0x1FFF 7800 - 0x1FFF 7A0F | 528 bytes |
| Option bytes | | | 0x1FFF C000 - 0x1FFF C00F | 16 bytes |

**Table 4.1:** STM32F407 flash memory organization

## 4.5. Application boot record

Aplication boot record is used to store meta data about the current user's application and new user's application. Meta data consists of:

- Checksum used for transmission,
- Application type used while transmitting,
- Length of application during transmission.

Boot record is also used to signalize that update of the application is needed to the bootloader. Flag is set when new application is successfully transmitted.

Listing 4.1 and Listing 4.2 show modifications added to the linker file needed to add the boot record. Address 0x800C000 is the starting address of sector 3 of the flash memory.

```
/* Specify the memory areas */
MEMORY
{
RAM (xrw)     : ORIGIN = 0x20000000, LENGTH = 128K
CCMRAM (rw)     : ORIGIN = 0x10000000, LENGTH = 64K
/* Allow bootloader only first 3 sectors */
```

```
FLASH (rx)     : ORIGIN = 0x8000000, LENGTH = 48K
/* Allow sector 3 for app boot record */
SEC3 (rx)             : ORIGIN = 0x800C000, LENGTH = 16K
}
```

**Listing 4.1:** Memory areas from the linker file.

```
 /* Application boot record */
 .appbr 0x800C000 (NOLOAD):
 {
   . = ALIGN(4);
   _sappbr = .;
   *(.appbr)
   *(.appbr*)

   . = ALIGN(4);
   _eappbr = .;
 } >SEC3
```

**Listing 4.2:** Application boot record from the linker file.

## 4.6. User application modifications

On the start of every STM32F407 program is a vector table. Vector table contains numerous interrupt and exception vectors. List of all vectors is avaliable in [3, p. 372]. On start up the program calls the vector on the address 4, the name of that vector is fittingly Reset handler. But before calling the reset handler main stack pointer(MSP) is set from the address 0.

Because the program expects the main stack pointer and reset handler vector to be on the start of the program vector offset register(VTOR) is available. Vector offset register is simply added onto the flash memory base address to allow multiple programs in the same flash memory. Perfect for writing a bootloader!

To sum up, before bootloader jumps to the user application it must set the MSP to the one of the user's application then it jumps to the application's reset handler. Vector offset register can be set be the bootloader or in the user's application, former is chosen in this project.

## 4.7. Command reference

Important notices:

- Every execute of a command must end with \r \n
- Commands are case insensitive
- On error bootloader returns "ERROR:<Explanation of error>"
- Optional parameters are surrounded with [] e.g. [example]

List of all commands:

- version - Gets a version of the bootloader
- help - Makes life easier
- reset - Resets the microcontroller
- cid - Gets chip identification number
- get-rdp-level - Gets read protection [3, p. 93]
- jump-to - Jumps to a requested address
- flash-erase - Erases flash memory
- flash-write - Writes to flash memory
- mem-read - Read bytes from memory
- update-act - Updates active application from new application memory area
- update-new - Updates new application
- en-write-prot - Enables write protection per sector
- dis-write-prot - Disables write protection per sector
- get-write-prot - Returns bit array of sector write protection
- exit - Exits the bootloader and starts the user application

### 4.7.1. version - Gets a version of the bootloader.

Parameters:

```
 - None
Execute command:

   > version

Response:
```

```
   v1.0
```

### 4.7.2. help - Makes life easier.

```
Parameters:

 -  None

Execute command:

   > help

Response:

   <List of all available commands and examples>
```

### 4.7.3. reset - Resets the microcontroller.

```
Parameters:

 - None

Execute command:

   > reset

Response:

   OK
```

### 4.7.4. cid - Gets chip identification number.

```
Parameters:

 - None

Execute command:
```

```
    > cid

Response:

    0x413
```

### 4.7.5. get-rdp-level - Gets read protection [3, p. 93]

```
Parameters:

  - None

Execute command:

    > get-rdp-level

Response:

    level 0
```

### 4.7.6. jump-to - Jumps to a requested address.

```
Parameters:

- addr - Address to jump to in hex format (e.g. 0x12345678), 0x can be
    omitted

Execute command:

    > jump-to addr=0x87654321

Response:

    OK
```

### 4.7.7. flash-erase - Erases flash memory.

```
Parameters:
```

- type - Defines type of flash erase. "mass" erases all sectors, "sector" erases only selected sectors

- sector - First sector to erase. Bootloader is on sectors 0, 1 and 2. Not needed with mass erase

- count - Number of sectors to erase. Not needed with mass erase

Execute command:

```
> flash-erase sector=3 type=sector count=4
```

Response:

```
OK
```

### 4.7.8. flash-write - Writes to flash memory.

Parameters:

- start - Starting address in hex format (e.g. 0x12345678), 0x can be omitted

- count - Number of bytes to write, without checksum. Chunk size: 5120

- [cksum] - Defines the checksum to use. If not present no checksum is assumed. WARNING: Even if checksum is wrong data will be written into flash memory!

  - "sha256" - Gives best protection (32 bytes), slowest, uses software implementation

  - "crc32" - Medium protection (4 bytes), fast, uses hardware implementation. Settings in [Apendix A](#apend_a)

  - "no" - No protection, fastest

Note:

When using crc-32 checksum sent data has to be divisible by 4

Execute command:

> flash-write start=0x87654321 count=64 cksum=crc32

Response:

chunks:1

chunk:0|length:64|address:0x87654321

ready

Send bytes:

<64 bytes>

Response:

chunk OK

checksum|length:4

ready

Send checksum:

<4 bytes>

Response:

OK

### 4.7.9. mem-read - Read bytes from memory.

Parameters:

- start - Starting address in hex format (e.g. 0x12345678), 0x can be

```
    omitted

- count - Number of bytes to read

Execute command:

    > mem-read start=0x87654321 count=3

Response:

    <3 bytes starting from the address 0x87654321>

Note:
- Entering invalid read address crashes the program and reboot is required.
```

### 4.7.10. update-act - Updates active application from new application memory area.

```
Parameters:
- [force] - Forces update even if not needed

   - "true" - Force the update

   - "false" - Don't force the update


Execute command:

    > update-act force=true

Response:

    No update needed for user application
    Updating user application
    OK
```

### 4.7.11. update-new - Updates new application.

```
Parameters:
```

- count - Number of bytes to write, without checksum. Chunk size: 5120

- type - Type of application coding

    - "bin" - Binary format (.bin)

    - "hex" - Intel hex format (.hex)

    - "srec" - Motorola S-record format (.srec)

- [cksum] - Defines the checksum to use. If not present no checksum is assumed. WARNING: Even if checksum is wrong data will be written into flash memory!

    - "sha256" - Gives best protection (32 bytes), slowest, uses software implementation

    - "crc32" - Medium protection (4 bytes), fast, uses hardware implementation. Settings in [Apendix A](#apend_a)

    - "no" - No protection, fastest

Execute command:

```
> update-new count=4 type=bin cksum=sha256
```

Response:

```
chunks:1

chunk:0|length:4|address:0x08080000

ready
```

Send bytes:

```
<4 bytes>
```

```
Response:

    chunk OK

    checksum|length:32

    ready

Send checksum:

     <32 bytes>

Response:

    OK
```

### 4.7.12. en-write-prot - Enables write protection per sector.

```
Parameters:

- mask - Mask in hex form for sectors where LSB corresponds to sector 0

Execute command:

    > en-write-prot mask=0xFF0

Response:

    OK
```

### 4.7.13. dis-write-prot - Disables write protection per sector.

```
Parameters:

- mask - Mask in hex form for sectors where LSB corresponds to sector 0

Execute command:

    > dis-write-prot mask=0xFF0
```

```
Response:

    OK
```

### 4.7.14. get-write-prot - Returns bit array of sector write protection.

Parameters:

```
- None

Execute command:

    > get-write-prot

Response:

    0b100000000010
```

### 4.7.15. exit - Exits the bootloader and starts the user application.

```
Parameters:

- None

Execute command:

    > exit

Response:

    Exiting
```

# 5. Conclusion

In this thesis a functional safety overview was presented.

**TODO**

# Bibliography

[1] Bootloader: What you need to know about the system boot manager. URL https://www.ionos.com/digitalguide/server/configuration/what-is-a-bootloader/.

[2] Briefing paper: Functional safety essential to overall safety. URL https://basecamp.iec.ch/download/functional-safety-essential-to-overall-safety/.

[3] *STM32F407 reference manual*. URL https://www.st.com/resource/en/reference_manual/dm00031020-stm32f405-415-stm32f407-417-stm32f427-437-and-stm32f
pdf.

[4] Michael Barr. Barr-c:2018 embedded c coding standard. URL https://barrgroup.com/sites/default/files/barr_c_coding_standard_2018.pdf.

**Software and Hardware Architecture for Redundant Embedded Systems**

**Abstract**

Abstract.

**Keywords:** Keywords.

**Programska i sklopovska arhitektura redundantnih ugradbenih računalnih sustava**

**Sažetak**

Sažetak.

**Ključne riječi:** Ključne riječi, odvojene zarezima.