# Audit Policy for OSTC

## Table of contents

## 1 Introduction

In OSTC, we believe in building true open source products. “True open source” does not mean identifying the problem, building the solution and donating that entire solution to the world. Rather, “true open source” is about **collaboration**, it is about **sharing** and **discussing ideas, plans and roadmaps** with others.

“True open source” is about **active and responsible members** of a community who share some **common fundamental values**: the freedom to use, study, share and improve software programs; the freedom of choosing technologies based only on their features and quality, and not because of vendor lock-in strategies; the value of interoperability, as a means to achieve such freedom; the values of shared learning, peer review and meritocracy, as a means to enhance developers’ skills – and get better software, too; the value of reusing others’ code while respecting their rights, in order to build a true software commons; the value of transparency, to share control on technology and protect everyone’s digital sovereignty.

This policy is about three of the most important values that we discussed above; i.e. to be compliant while reusing others' code, protect everyone's digital sovereignty, and make sure that our downstream users get a truly open source product.

## 2 Scope

### Objective Scope

This policy covers **Eclipse Oniro Project** (herein after 'Project') and any other open source projects to which OSTC contributes. As of now, the policy is framed in the context of the Project, as it is the only open source project to which OSTC contributes.

### Subjective Scope

This policy is applicable to the source code audits done by auditors, collaborators and any other individuals or entities connected to source code audit of software incorporated in to the Project.

## 3 Glossary

Some of the definitions in this section are taken from Section 2 of the OpenChain Specification 2.0, Copyright 2016-2019 Linux Foundation, licensed under CC-BY-4.0

**Audit Team** The team that does the source code audit of own code and third party code using Open Source auditing tools.

**Legal Team** The team of lawyers who, drafted the Project's IP policy, reviews the decisions made by the Audit Team as per need, provide right advice, and make critical legal decisions.

**Upstream, downstream** Direction from and to which software and other information or technology flows in a chain of interaction from the originating artifacts and their modifications until they reach the final distribution outlet. If entity A provides technology to entity B, that receives and transforms it, A is upstream to B and B is downstream to A.

**Compliance artifacts** [from Openchain 2.0 defintion] a collection of artifacts that represent the output of the OpenChain-compliant process for the published software. The collection may include (but is not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers, Open Source component bill of materials, and SPDX documents.

**Open Source License** In descending order of preference (a) an OSI-approved license, or (b) a license qualifying as free software according to the list published by the Free Software Foundation (FSF), or (c) a license falling within the Open Source Definition and/or within the FSF definition of Free Software, **but** which is neither OSI-approved nor expressly listed by FSF (note that this latter option requires a previous assessment by the internal Legal Team to be considered “open source”).

**Proprietary blobs** Binary executable code owned by proprietary third party vendors.

**license text reference** Reference to a license. It could be a standard english sentence refering to the license of a file, or SPDX standardized short identifier.

**documentation files** Files that are part of the documentation of an open source component.

**FOSSology** FOSSology is a open source license compliance software system and toolkit. As a toolkit you can run license, copyright and export control scans from the command line. As a system, a database and web ui are provided to give you a compliance workflow. License, copyright and export scanners are tools available to help with your compliance activities.

**ScanCode** ScanCode is a tool to scan code and detect licenses, copyrights and more.

**Compliance Artifacts** a collection of artifacts that represent the output of the Program for the Supplied Software.The collection may include (but is not limited to) one or more of the following: source code, attribution notices,copyright notices, copy of licenses, modification notifications, written offers, Open Source component bill of materials, and SPDX documents.

**Identified Licenses** a set of Open Source Software licenses identified as a result of following an appropriate method of identifying Open Source components from which the Supplied Software is comprised.

**SPDX** the format standard created by the Linux Foundation’s SPDX (Software Package Data Exchange) WorkingGroup for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at www.spdx.org.

# 4 The audit process

It is critical for the Project to make sure that the licenses of the source code and binaries that are distributed are those that comply with the Open Source Definition — in brief, they allow software to be freely used, modified, and shared. There could be exceptions though, that needs to be considered according to situations. The audit process has an important role in ensuring this.

The source code audit process in OSTC ensures that information about third party software is available to the downstream users, and all software distributables are accompanied by corresponding SBOMS, that comply with the existing accepted industry standards. In the Project, we reuse the existing tools available in yocto/bitbake, modified to suit our requirements, to collect the source code of all third party components consumed, for license audits. The tool that we developed based on yocto/bitbake is called Aliens4Friends, and the next section briefs about the tool.

The source code of third party components are uploaded to Fossology with the help of Aliens4Friends and automated using gitlab runners. The Fossology agents for unpacking and license identification are run on the source code, triggered by Alines4Friends. Usually, The Audit Team does an initial analysis of the uploaded components, and identify, report and initiate discussions on very obvious license issues, without going in to the in-depth analysis of the source code. The next step is to analyse the source code of each component in detail by navigating through the files and validating the scanner identified licenses. This step is needed because Fossology scanners identify licenses based on keywords and text matches that can introduce false positives as well.

Obligations, restrictions and rights granted by most prevalent open source Licenses (as those listed in ‘Choose a License’ website) are reviewed and documented by the Audit Team using functionalities provided by our license scanning tool, and are included in each software component’s internal report generated through such tool. For uncommon open source licenses (and for uncommon variants of common licenses), an assessment by the Legal Team is required, which will be managed through the OSS issue tracker described in the Appendix (the “OSS IssueTracker”); issues in this respect should be opened by any OSTC team member who encounters an uncommon Identified License that appears not to have been reviewed yet in the OSS Issue Tracker or in the OSS wiki described in the Appendix (the“OSS Wiki”). The final outcome of the assessment will be included in the database of the license scanning tool by the Audit Team.

Please see the 'Getting started with Fossology' document to know how a source code audit is done in Fossology with detailed step by step explanation.

## Aliens4Friends

It is a tool for Software Composition Analysis (SCA), expressly designed to analyze Yocto/bitbake builds -- but it could be usefully adopted in any software composition context where a package manager is missing, and where source code provenance and license/copyright metadata are often missing, messy, uncertain and/or imprecise. The tool uploads source code packages to Fossology, integrate ScanCode as a scanner along with Fossology, find matching Debian packages and import their license and copyright metadata to Fossology, schedule scan agents like ojo for REUSE-compliant packages, collects SBOM in SPDX format, and elaborate the statistics on progress and results of the audit work and show them in a dashboard. More information about the tool could be found in the git repository.

The Aliens4Friends tool applies the license information of packages for which a matching Debian package is found, to files of the corresponding source package in Fossology. This reduces the effort and time required for audit work. The Audit Team may have to audit and apply decision only on files that do not have a license decision applied.

The following section lists different kinds of license texts or files that the Audit Team comes across when they audit source code, and the recommended way to identify each one of them. The types of license texts and files are not exhaustive. There would be updates to this document as and when a new type of license or file is audited.

## Audit of most common types of files found in source code packages

*Source code files*

Some of the most common source code files have the extensions .c, .cpp, .java, .py etc. Those files needs to be audited and decisions related to applicability of license texts or references found on such files should be made, as they would be used by downstream users like device makers when they distribute thier applications or products.

Some files that contain source code may be a part of Example folders or Test folders. From the perspective of auditing of Project, such files are treated like other source files, as bundling of such files for distribution could be mandatory in many use cases of downstream users.

The source code files should be audited in the same way as detailed in the Fossology Basic Workflow.

*Build files*

From the perspective of source code audits in Project, such files are treated like other source files, as bundling of such files for distribution could be mandatory in many use cases of downstream users.

*Documentation files*

From the perspective of source code audits in Project, such files are treated like other source files, as bundling of such files for distribution could be mandatory in many use cases of downstream users.

## Audit of special non-code files found in source code packages

*Image files*

The Audit Team checks the folders in which the image files are present, or the heirarchical parent folders, for information on the license of the images. e.g. A README file could be present, or information about licenses of the files may be included in the README file of the project. If not found, the team does research in the internet to find out information about licenses or details of copyright holders of the images. The Audit Team, if needed, consults the legal team before making a decision. If no relevant information could be found, that should be documented with details of the research done.

*Sound files*

The Audit Team checks the folders in which the sound files are present, or the heirarchical parent folders, for information on the license of the sound files. e.g. A README file could be present, or information about licenses of the files may be included in the README file of the project. If not found, the team does research in the internet to find out information about licenses or details of copyright holders of the sound files. The Audit Team, if needed, consults the legal team before making a decision. If no relevant information could be found, that should be documented with details of the research done.

*Font files*

From the perspective of source code audits in Project, such files are treated like other source files when license information is present in the font files. If no license information is present, the Audit Team checks the folders in which the font files are present, or the heirarchical parent folders, for information on the license of the font files. e.g. A README file could be present, or information about licenses of the files may be included in the README file of the project. If not found, the team does research in the internet to find out information about licenses or details of copyright holders of the font files. The Audit Team, if needed, consults the legal team before making a decision. If no relevant information could be found, that should be documented with details of the research done.

*Proprietary blobs*

The Audit Team checks the heirarchical parent folders for any license information of the proprietary blobs. If not found, the team does research in the internet to find out information about licenses or details of copyright holders of the propietary blobs. The Audit Team, if needed, consults the legal team before making a decision.

Project projects are generally intended to be released as source only distributions. Distribution of application and/or library binaries should be generally avoided within Project projects; however, some binary blobs could have to be distributed along with Project, to enable compatibility with certain hardware devices and components. License obligations, restrictions and rights related to such binary blobs shall be always reviewed and assessed by the Legal Team. Since the Project is intended to be implemented downstream by device makers, who will typically perform a binary distribution of modified parts of such software, Project working group commits to provide them with some basic assessment and information on license obligations, restrictions in the context of a typical binary/firmware distribution, including information about the existence and the license conditions of possible third party binary blobs.

**Note**: Fossology scanners identify licenses by text matches and keyword matches. Some of the image files, sound files, font files, proprietary blobs etc. may not contain license texts or keywords. Fossology scanners won't consider such files as 'to be audited'. So, the Audit Team may not come across such files during audit. This may cause such files to go without a license decision. To avoid this, and to bring such files for auditing, we have included an automation in our compliance pipeline, to stamp a custom license identifier to such files. During the audit, when the Audit Team finds files with those identifiers, they should follow the respective audit process for the file type, as mentioned in this section.

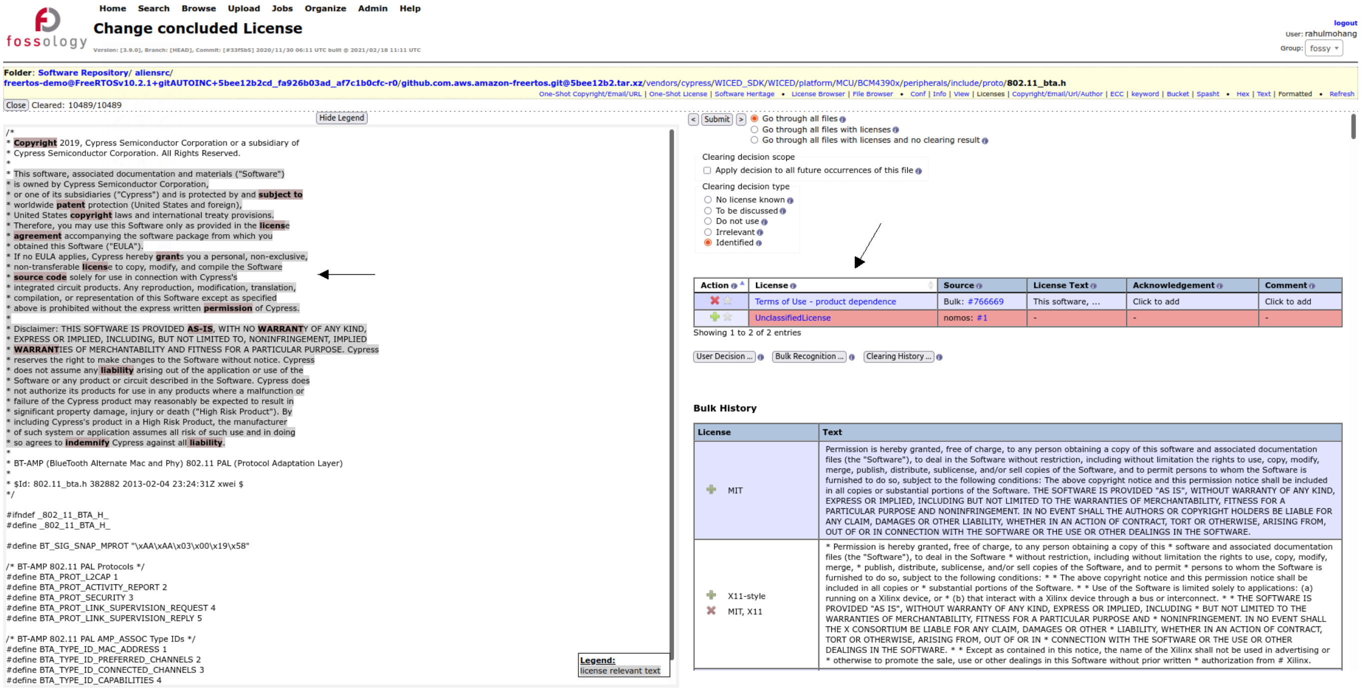
### Audit of files with reference to non open source licenses

One of the main focus areas for audit of third party code in Project is to identify, document, and decide on the distribution of source code files with licenses that do not provide all the freedoms that are supposed to be guaranteed by an open source license. The importance of identifying such licenses and deciding on their usage is critical for a project that is fully open source.

There are different kinds of such license references. e.g.

*Product dependent licenses*

Licenses that grant rights for usage and further distribution based on usage on a particular type of product do not satisfy the criterion 8 of the Open Source Definition. The Audit team identifies such licenses found in the audited source code and documents it for further discussions with the development team. A custom license identifier called 'Terms of Use - product dependence' is used to identify such licenses. Please see below, a screenshot of such an identification in Fossology:


fossology
Home Search Browse Upload Jobs Organize Admin Help
logout
One-Shot Copyright/Email/URL | One-Shot License | Software Heritage • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | keyword | Bucket | Spasht • Hex | Text | Formatted • Refresh
Close
Hide Legend
< Submit >
User Decision ... Bulk Recognition ... Clearing History ...

**Change concluded License**

Version: [3.9.0], Branch: [HEAD], Commit: [#33f5b5] 2020/11/30 06:11 UTC built @ 2021/02/18 11:11 UTC

User: rahulmohang
Group: fossy

Folder: Software Repository/ aliensrc/
freertos-demo@FreeRTOSv10.2.1+gitAUTOINC+5bee12b2cd_fa926b03ad_af7c1b0cfc-r0/github.com.aws.amazon-freertos.git@5bee12b2.tar.xz/vendors/cypress/WICED_SDK/WICED/platform/MCU/BCM4390x/peripherals/include/proto/802.11_bta.h

Cleared: 10489/10489

```
/*
* Copyright 2019, Cypress Semiconductor Corporation or a subsidiary of
* Cypress Semiconductor Corporation. All Rights Reserved.
*
* This software, associated documentation and materials ("Software")
* is owned by Cypress Semiconductor Corporation,
* or one of its subsidiaries ("Cypress") and is protected by and subject to
* worldwide patent protection (United States and foreign),
* United States copyright laws and international treaty provisions.
* Therefore, you may use this Software only as provided in the license
* agreement accompanying the software package from which you
* obtained this Software ("EULA").
* If no EULA applies, Cypress hereby grants you a personal, non-exclusive,
* non-transferable license to copy, modify, and compile the Software
* source code solely for use in connection with Cypress's
* integrated circuit products. Any reproduction, modification, translation,
* compilation, or representation of this Software except as specified
* above is prohibited without the express written permission of Cypress.
*
* Disclaimer: THIS SOFTWARE IS PROVIDED AS-IS, WITH NO WARRANTY OF ANY KIND,
* EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, NONINFRINGEMENT, IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cypress
* reserves the right to make changes to the Software without notice. Cypress
* does not assume any liability arising out of the application or use of the
* Software or any product or circuit described in the Software. Cypress does
* not authorize its products for use in any products where a malfunction or
* failure of the Cypress product may reasonably be expected to result in
* significant property damage, injury or death ("High Risk Product"). By
* including Cypress's product in a High Risk Product, the manufacturer
* of such system or application assumes all risk of such use and in doing
* so agrees to indemnify Cypress against all liability.
*
* BT-AMP (BlueTooth Alternate Mac and Phy) 802.11 PAL (Protocol Adaptation Layer)
*
* $Id: 802.11_bta.h 382882 2013-02-04 23:24:31Z xwei $
*/

#ifndef _802_11_BTA_H_
#define _802_11_BTA_H_

#define BT_SIG_SNAP_MPROT "\xAA\xAA\x03\x00\x19\x58"

/* BT-AMP 802.11 PAL Protocols */
#define BTA_PROT_L2CAP 1
#define BTA_PROT_ACTIVITY_REPORT 2
#define BTA_PROT_SECURITY 3
#define BTA_PROT_LINK_SUPERVISION_REQUEST 4
#define BTA_PROT_LINK_SUPERVISION_REPLY 5

/* BT-AMP 802.11 PAL AMP_ASSOC Type IDs */
#define BTA_TYPE_ID_MAC_ADDRESS 1
#define BTA_TYPE_ID_PREFERRED_CHANNELS 2
#define BTA_TYPE_ID_CONNECTED_CHANNELS 3
#define BTA_TYPE_ID_CAPABILITIES 4
```

Legend:
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope
□ Apply decision to all future occurrences of this file

Clearing decision type
○ No license known
○ To be discussed
○ Do not use
○ Irrelevant
● Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|---|---|---|---|---|---|
| ✗ ☆ | Terms of Use - product dependence | Bulk: #766669 | This software, ... | Click to add | Click to add |
| + ☆ | UnclassifiedLicense | nomos: #1 | - | - | - |

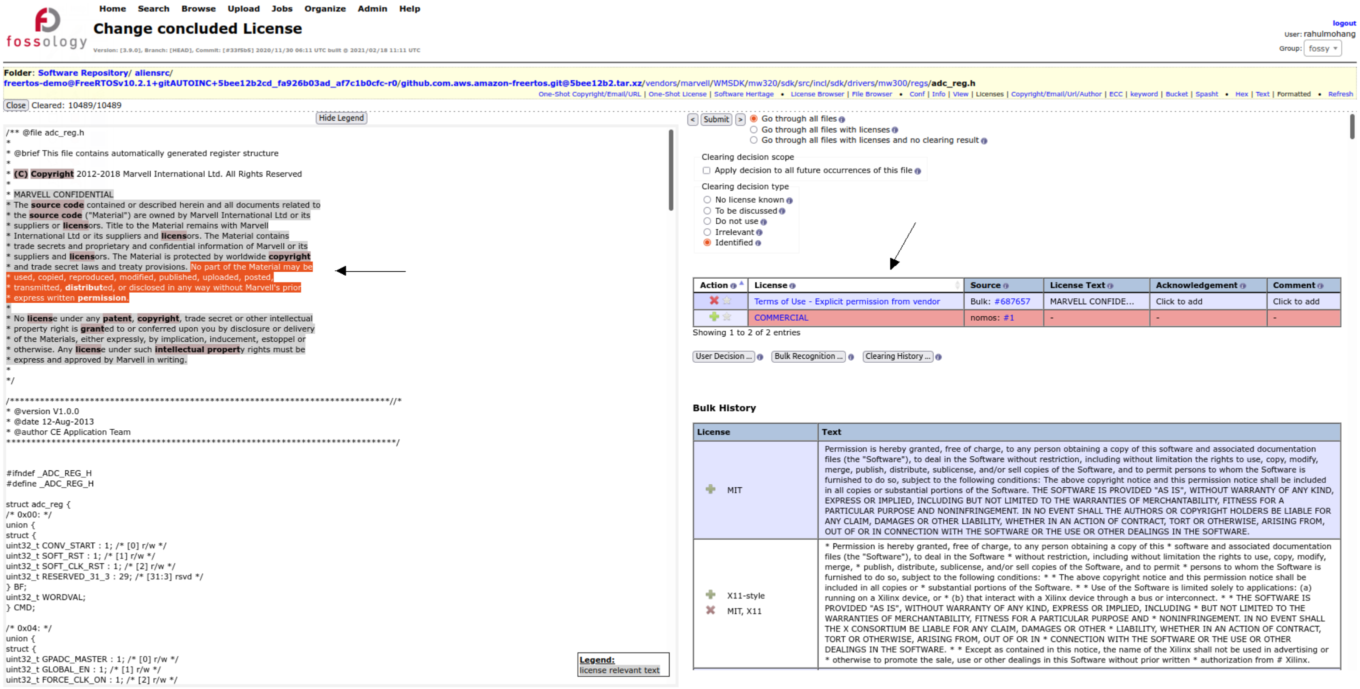
Showing 1 to 2 of 2 entries

**Bulk History**

| License | Text |
|---|---|
| + MIT | Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. |
| + X11-style<br>✗ MIT, X11 | * Permission is hereby granted, free of charge, to any person obtaining a copy of this * software and associated documentation files (the "Software"), to deal in the Software * without restriction, including without limitation the rights to use, copy, modify, merge, * publish, distribute, sublicense, and/or sell copies of the Software, and to permit * persons to whom the Software is furnished to do so, subject to the following conditions: * * The above copyright notice and this permission notice shall be included in all copies or * substantial portions of the Software. * * Use of the Software is limited solely to applications: (a) running on a Xilinx device, or * (b) that interact with a Xilinx device through a bus or interconnect. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING * BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND * NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN * CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. * * Except as contained in this notice, the name of the Xilinx shall not be used in advertising or * otherwise to promote the sale, use or other dealings in this Software without prior written * authorization from # Xilinx. |

### *Licenses that require explicit permission from vendor*

Licenses that restrict usage and distribution without a written consent by the owner of the copyright to the software do not satisfy the criterion 7 of Open Source Definition. The Audit team identifies such licenses found in the audited source code and documents it for further discussions with the development team. A custom license identifier called 'Terms of Use - Explicit permission from vendor' is used to identify such licenses. Please see below, a screenshot of such an identification in Fossology:


fossology
Home Search Browse Upload Jobs Organize Admin Help
logout
One-Shot Copyright/Email/URL | One-Shot License | Software Heritage • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | keyword | Bucket | Spasht • Hex | Text | Formatted • Refresh
Close
Hide Legend
< Submit >
User Decision ... Bulk Recognition ... Clearing History ...

**Change concluded License**

Version: [3.9.0], Branch: [HEAD], Commit: [#33f5b5] 2020/11/30 06:11 UTC built @ 2021/02/18 11:11 UTC

User: rahulmohang
Group: fossy

Folder: Software Repository/ aliensrc/
freertos-demo@FreeRTOSv10.2.1+gitAUTOINC+5bee12b2cd_fa926b03ad_af7c1b0cfc-r0/github.com.aws.amazon-freertos.git@5bee12b2.tar.xz/vendors/marvell/WMSDK/mw320/sdk/src/incl/sdk/drivers/mw300/regs/adc_reg.h

Cleared: 10489/10489

```
/** @file adc_reg.h
*
* @brief This file contains automatically generated register structure
*
* (C) Copyright 2012-2018 Marvell International Ltd. All Rights Reserved
*
* MARVELL CONFIDENTIAL
* The source code contained or described herein and all documents related to
* the source code ("Material") are owned by Marvell International Ltd or its
* suppliers or licensors. Title to the Material remains with Marvell
* International Ltd or its suppliers and licensors. The Material contains
* trade secrets and proprietary and confidential information of Marvell or its
* suppliers and licensors. The Material is protected by worldwide copyright
* and trade secret laws and treaty provisions. No part of the Material may be
* used, copied, reproduced, modified, published, uploaded, posted,
* transmitted, distributed, or disclosed in any way without Marvell's prior
* express written permission.
*
* No license under any patent, copyright, trade secret or other intellectual
* property right is granted to or conferred upon you by disclosure or delivery
* of the Materials, either expressly, by implication, inducement, estoppel or
* otherwise. Any license under such intellectual property rights must be
* express and approved by Marvell in writing.
*
*/

/****************************************************************************//*
* @version V1.0.0
* @date 12-Aug-2013
* @author CE Application Team
*****************************************************************************/


#ifndef _ADC_REG_H
#define _ADC_REG_H

struct adc_reg {
/* 0x00: */
union {
struct {
uint32_t CONV_START : 1; /* [0] r/w */
uint32_t SOFT_RST : 1; /* [1] r/w */
uint32_t SOFT_CLK_RST : 1; /* [2] r/w */
uint32_t RESERVED_31_3 : 29; /* [31:3] rsvd */
} BF;
uint32_t WORDVAL;
} CMD;

/* 0x04: */
union {
struct {
uint32_t GPADC_MASTER : 1; /* [0] r/w */
uint32_t GLOBAL_EN : 1; /* [1] r/w */
uint32_t FORCE_CLK_ON : 1; /* [2] r/w */
```

Legend:
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope
□ Apply decision to all future occurrences of this file

Clearing decision type
○ No license known
○ To be discussed
○ Do not use
○ Irrelevant
● Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|---|---|---|---|---|---|
| ✗ ☆ | Terms of Use - Explicit permission from vendor | Bulk: #687657 | MARVELL CONFIDE... | Click to add | Click to add |
| + ☆ | COMMERCIAL | nomos: #1 | - | - | - |

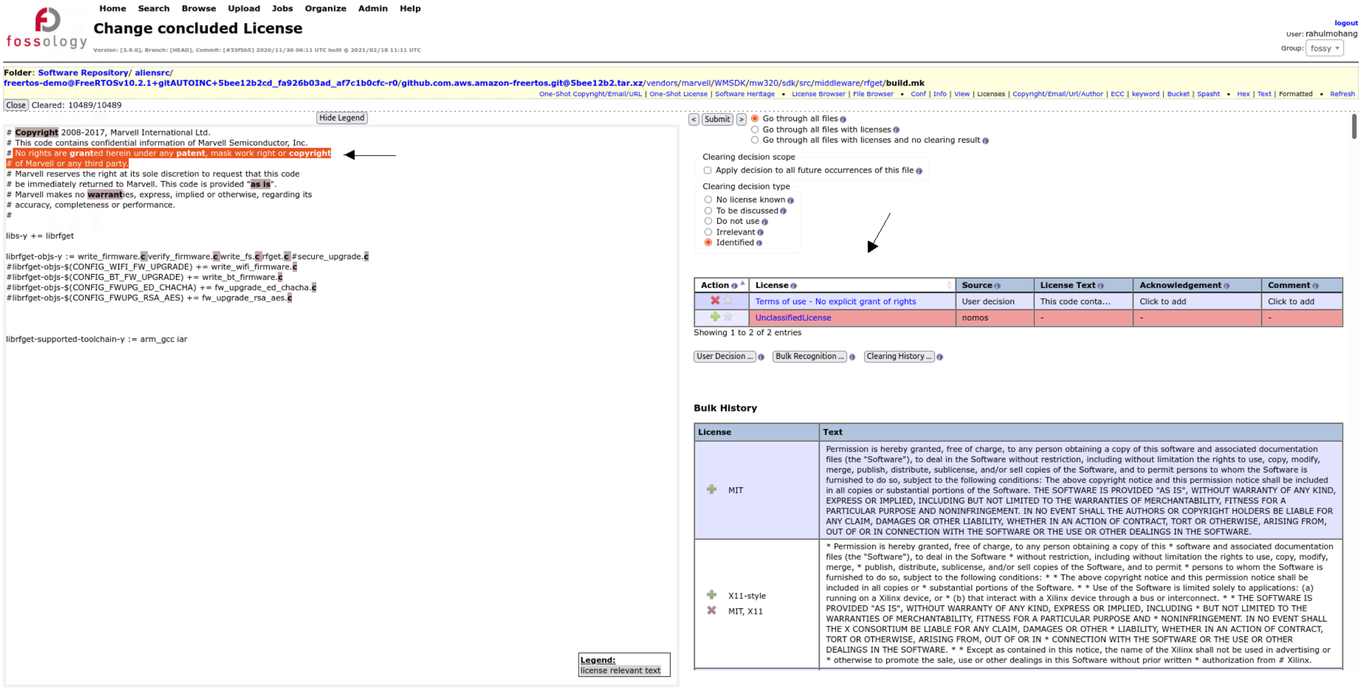
Showing 1 to 2 of 2 entries

**Bulk History**

| License | Text |
|---|---|
| + MIT | Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. |
| + X11-style<br>✗ MIT, X11 | * Permission is hereby granted, free of charge, to any person obtaining a copy of this * software and associated documentation files (the "Software"), to deal in the Software * without restriction, including without limitation the rights to use, copy, modify, merge, * publish, distribute, sublicense, and/or sell copies of the Software, and to permit * persons to whom the Software is furnished to do so, subject to the following conditions: * * The above copyright notice and this permission notice shall be included in all copies or * substantial portions of the Software. * * Use of the Software is limited solely to applications: (a) running on a Xilinx device, or * (b) that interact with a Xilinx device through a bus or interconnect. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING * BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND * NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN * CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. * * Except as contained in this notice, the name of the Xilinx shall not be used in advertising or * otherwise to promote the sale, use or other dealings in this Software without prior written * authorization from # Xilinx. |

### *Licenses that do not have explicit grant of rights of use*

Licenses that do not have an explicit statement that grants the rights to use and distribution may restrict the Project as well as the downstream users from making use of the software licensed under such licenses, in any way. The Audit team identifies such licenses found in the audited source code and documents it for further discussions with the development team. A custom license identifier called 'Terms of Use - No explicit grant of rights' is used to identify such licenses. Please see below, a screenshot of such an identification in Fossology:


Home Search Browse Upload Jobs Organize Admin Help
fossology
logout
User: rahulmohang
Group: fossy
One-Shot Copyright/Email/URL | One-Shot License | Software Heritage • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | keyword | Bucket | Spasht • Hex | Text | Formatted • Refresh
Close
Hide Legend
< Submit >
User Decision ... Bulk Recognition ... Clearing History ...

Change concluded License

Version: [3.9.0], Branch: [HEAD], Commit: [#33f5b5] 2020/11/30 06:11 UTC built @ 2021/02/18 11:11 UTC

Folder: Software Repository/ aliensrc/
freertos-demo@FreeRTOSv10.2.1+gitAUTOINC+5bee12b2cd_fa926b03ad_af7c1b0cfc-r0/github.com.aws.amazon-freertos.git@5bee12b2.tar.xz/vendors/marvell/WMSDK/mw320/sdk/src/middleware/rfget/build.mk

Cleared: 10489/10489

```
# Copyright 2008-2017, Marvell International Ltd.
# This code contains confidential information of Marvell Semiconductor, Inc.
# No rights are granted herein under any patent, mask work right or copyright
# of Marvell or any third party.
# Marvell reserves the right at its sole discretion to request that this code
# be immediately returned to Marvell. This code is provided "as is".
# Marvell makes no warranties, express, implied or otherwise, regarding its
# accuracy, completeness or performance.
#

libs-y += librfget

librfget-objs-y := write_firmware.c verify_firmware.c write_fs.c rfget.c #secure_upgrade.c
#librfget-objs-$(CONFIG_WIFI_FW_UPGRADE) += write_wifi_firmware.c
#librfget-objs-$(CONFIG_BT_FW_UPGRADE) += write_bt_firmware.c
#librfget-objs-$(CONFIG_FWUPG_ED_CHACHA) += fw_upgrade_ed_chacha.c
#librfget-objs-$(CONFIG_FWUPG_RSA_AES) += fw_upgrade_rsa_aes.c



librfget-supported-toolchain-y := arm_gcc iar
```

Legend:
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope
□ Apply decision to all future occurrences of this file

Clearing decision type
○ No license known
○ To be discussed
○ Do not use
○ Irrelevant
● Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|---|---|---|---|---|---|
| ✖ ☆ | Terms of use - No explicit grant of rights | User decision | This code conta... | Click to add | Click to add |
| ✚ ☆ | UnclassifiedLicense | nomos | - | - | - |

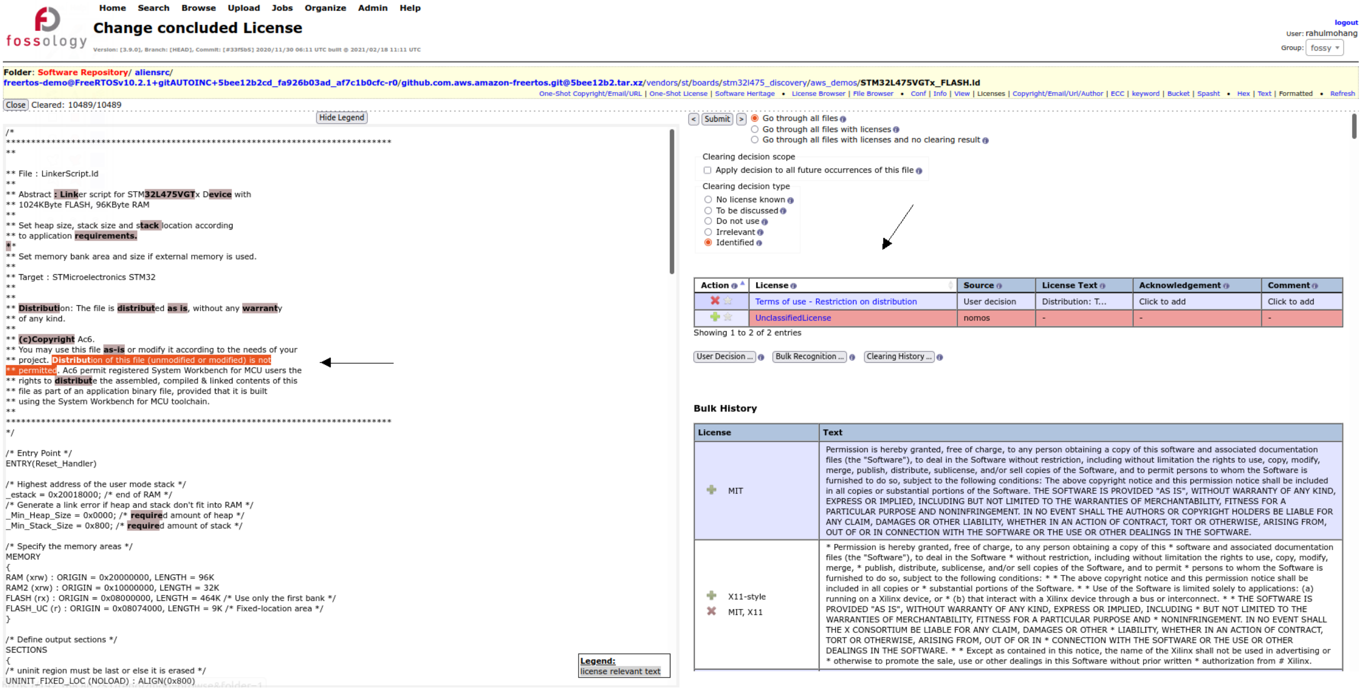
Showing 1 to 2 of 2 entries

**Bulk History**

| License | Text |
|---|---|
| ✚ MIT | Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. |
| ✚ X11-style<br>✖ MIT, X11 | * Permission is hereby granted, free of charge, to any person obtaining a copy of this * software and associated documentation files (the "Software"), to deal in the Software * without restriction, including without limitation the rights to use, copy, modify, merge, * publish, distribute, sublicense, and/or sell copies of the Software, and to permit * persons to whom the Software is furnished to do so, subject to the following conditions: * * The above copyright notice and this permission notice shall be included in all copies or * substantial portions of the Software. * * Use of the Software is limited solely to applications: (a) running on a Xilinx device, or * (b) that interact with a Xilinx device through a bus or interconnect. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING * BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND * NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN * CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. * * Except as contained in this notice, the name of the Xilinx shall not be used in advertising or * otherwise to promote the sale, use or other dealings in this Software without prior written * authorization from # Xilinx. |

*Licenses that explicitly restricts distribution of software*

Licenses that explicitly restricts distribution of software in source code form or binary form do not satisfy the criterion 2 of the Open Source Definition. The Audit team identifies such licenses found in the audited source code and documents it for further discussions with the development team. A custom license identifier called 'Terms of Use - Explicit permission from vendor' is used to identify such licenses. Please see below, a screenshot of such an identification in Fossology:


Home Search Browse Upload Jobs Organize Admin Help
fossology
logout
User: rahulmohang
Group: fossy
One-Shot Copyright/Email/URL | One-Shot License | Software Heritage • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | keyword | Bucket | Spasht • Hex | Text | Formatted • Refresh
Close
Hide Legend
< Submit >
User Decision ... Bulk Recognition ... Clearing History ...

Change concluded License

Version: [3.9.0], Branch: [HEAD], Commit: [#33f5b5] 2020/11/30 06:11 UTC built @ 2021/02/18 11:11 UTC

Folder: Software Repository/ aliensrc/
freertos-demo@FreeRTOSv10.2.1+gitAUTOINC+5bee12b2cd_fa926b03ad_af7c1b0cfc-r0/github.com.aws.amazon-freertos.git@5bee12b2.tar.xz/vendors/st/boards/stm32l475_discovery/aws_demos/STM32L475VGTx_FLASH.ld

Cleared: 10489/10489

```
/*
*****************************************************************************
**

** File : LinkerScript.ld
**
** Abstract : Linker script for STM32L475VGTx Device with
** 1024KByte FLASH, 96KByte RAM
**
** Set heap size, stack size and stack location according
** to application requirements.
**
** Set memory bank area and size if external memory is used.
**
** Target : STMicroelectronics STM32
**
**
** Distribution: The file is distributed as is, without any warranty
** of any kind.
**
** (c)Copyright Ac6.
** You may use this file as-is or modify it according to the needs of your
** project. Distribution of this file (unmodified or modified) is not
** permitted. Ac6 permit registered System Workbench for MCU users the
** rights to distribute the assembled, compiled & linked contents of this
** file as part of an application binary file, provided that it is built
** using the System Workbench for MCU toolchain.
**
*****************************************************************************
*/

/* Entry Point */
ENTRY(Reset_Handler)

/* Highest address of the user mode stack */
_estack = 0x20018000; /* end of RAM */
/* Generate a link error if heap and stack don't fit into RAM */
_Min_Heap_Size = 0x0000; /* required amount of heap */
_Min_Stack_Size = 0x800; /* required amount of stack */

/* Specify the memory areas */
MEMORY
{
RAM (xrw) : ORIGIN = 0x20000000, LENGTH = 96K
RAM2 (xrw) : ORIGIN = 0x10000000, LENGTH = 32K
FLASH (rx) : ORIGIN = 0x08000000, LENGTH = 464K /* Use only the first bank */
FLASH_UC (r) : ORIGIN = 0x08074000, LENGTH = 9K /* Fixed-location area */
}

/* Define output sections */
SECTIONS
{
/* uninit region must be last or else it is erased */
UNINIT_FIXED_LOC (NOLOAD) : ALIGN(0x800)
```

Legend:
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope
□ Apply decision to all future occurrences of this file

Clearing decision type
○ No license known
○ To be discussed
○ Do not use
○ Irrelevant
● Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|---|---|---|---|---|---|
| ✖ ☆ | Terms of use - Restriction on distribution | User decision | Distribution: T... | Click to add | Click to add |
| ✚ ☆ | UnclassifiedLicense | nomos | - | - | - |

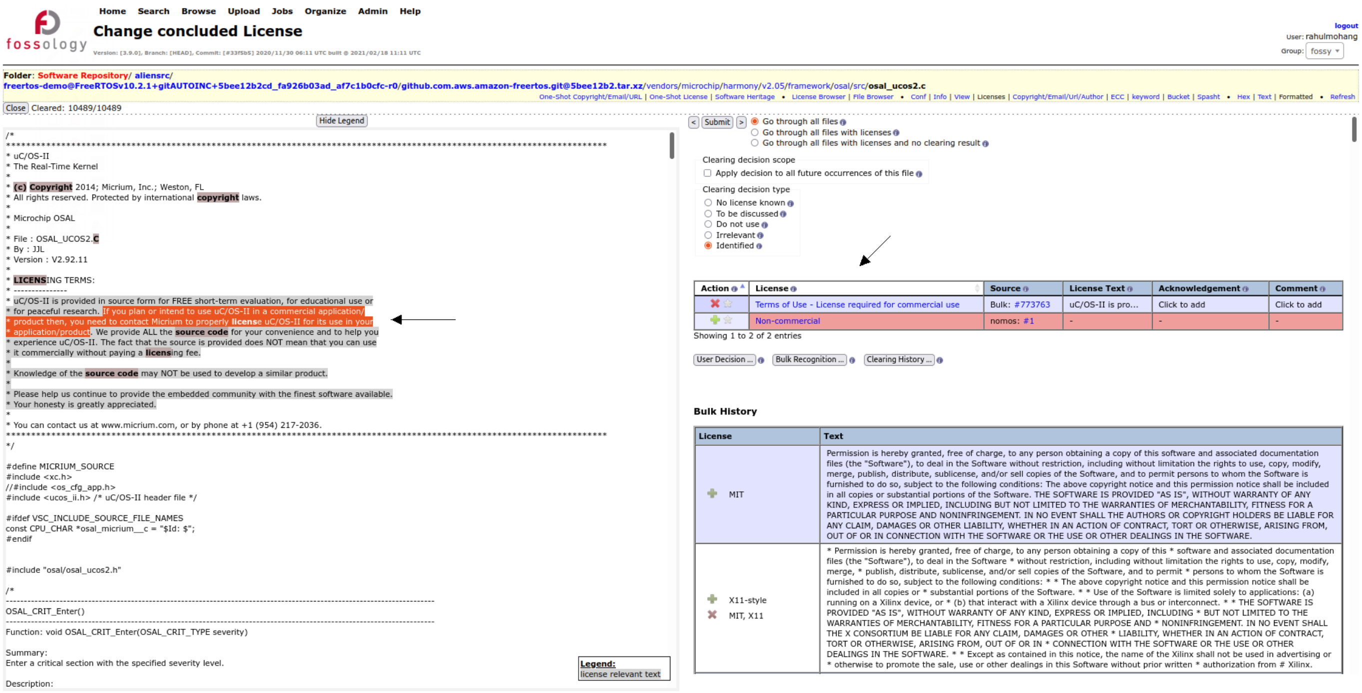
Showing 1 to 2 of 2 entries

**Bulk History**

| License | Text |
|---|---|
| ✚ MIT | Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. |
| ✚ X11-style<br>✖ MIT, X11 | * Permission is hereby granted, free of charge, to any person obtaining a copy of this * software and associated documentation files (the "Software"), to deal in the Software * without restriction, including without limitation the rights to use, copy, modify, merge, * publish, distribute, sublicense, and/or sell copies of the Software, and to permit * persons to whom the Software is furnished to do so, subject to the following conditions: * * The above copyright notice and this permission notice shall be included in all copies or * substantial portions of the Software. * * Use of the Software is limited solely to applications: (a) running on a Xilinx device, or * (b) that interact with a Xilinx device through a bus or interconnect. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING * BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND * NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN * CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. * * Except as contained in this notice, the name of the Xilinx shall not be used in advertising or * otherwise to promote the sale, use or other dealings in this Software without prior written * authorization from # Xilinx. |

*Licenses that demand additional permission to be taken for commercial distribution*

Licenses that, by written statement, demands additional license to be obtained for commercial use, that do not satisfy the criterion 1 of the Open Source Definition. The Audit team identifies such licenses found in the audited source code and documents it for further discussions with the development team. A custom license identifier called 'Terms of Use - License required for commercial use' is used to identify such licenses. Please see below, a screenshot of such an identification in Fossology:



**Change concluded License**

Version: [3.9.0], Branch: [HEAD], Commit: [#33f5b5] 2020/11/30 06:11 UTC built @ 2021/02/18 11:11 UTC

logout
User: rahulmohang
Group: fossy

Folder: Software Repository/ aliensrc/ freertos-demo@FreeRTOSv10.2.1+gitAUTOINC+5bee12b2cd_fa926b03ad_af7c1b0cfc-r0/github.com.aws.amazon-freertos.git@5bee12b2.tar.xz/vendors/microchip/harmony/v2.05/framework/osal/src/osal_ucos2.c

One-Shot Copyright/Email/URL | One-Shot License | Software Heritage • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | keyword | Bucket | Spasht • Hex | Text | Formatted • Refresh
Close
Hide Legend
< Submit >

Cleared: 10489/10489

```
/*
*********************************************************************************************************
* uC/OS-II
* The Real-Time Kernel
*
* (c) Copyright 2014; Micrium, Inc.; Weston, FL
* All rights reserved. Protected by international copyright laws.
*
* Microchip OSAL
*
* File : OSAL_UCOS2.C
* By : JJL
* Version : V2.92.11
*
* LICENSING TERMS:
* ---------------
* uC/OS-II is provided in source form for FREE short-term evaluation, for educational use or
* for peaceful research. If you plan or intend to use uC/OS-II in a commercial application/
* product then, you need to contact Micrium to properly license uC/OS-II for its use in your
* application/product. We provide ALL the source code for your convenience and to help you
* experience uC/OS-II. The fact that the source is provided does NOT mean that you can use
* it commercially without paying a licensing fee.
*
* Knowledge of the source code may NOT be used to develop a similar product.
*
* Please help us continue to provide the embedded community with the finest software available.
* Your honesty is greatly appreciated.
*
* You can contact us at www.micrium.com, or by phone at +1 (954) 217-2036.
*********************************************************************************************************
*/

#define MICRIUM_SOURCE
#include <xc.h>
//#include <os_cfg_app.h>
#include <ucos_ii.h> /* uC/OS-II header file */

#ifdef VSC_INCLUDE_SOURCE_FILE_NAMES
const CPU_CHAR *osal_micrium__c = "$Id: $";
#endif


#include "osal/osal_ucos2.h"

/*
-----------------------------------------------------------------------------------------------------------
OSAL_CRIT_Enter()
-----------------------------------------------------------------------------------------------------------
Function: void OSAL_CRIT_Enter(OSAL_CRIT_TYPE severity)

Summary:
Enter a critical section with the specified severity level.

Description:
```

**Legend:**
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope
☐ Apply decision to all future occurrences of this file

Clearing decision type
○ No license known
○ To be discussed
○ Do not use
○ Irrelevant
● Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|---|---|---|---|---|---|
| ✗ ☆ | Terms of Use - License required for commercial use | Bulk: #773763 | uC/OS-II is pro... | Click to add | Click to add |
| + ☆ | Non-commercial | nomos: #1 | - | - | - |

Showing 1 to 2 of 2 entries

**Bulk History**

| License | Text |
|---|---|
| + MIT | Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. |
| + X11-style<br>✗ MIT, X11 | * Permission is hereby granted, free of charge, to any person obtaining a copy of this * software and associated documentation files (the "Software"), to deal in the Software * without restriction, including without limitation the rights to use, copy, modify, merge, * publish, distribute, sublicense, and/or sell copies of the Software, and to permit * persons to whom the Software is furnished to do so, subject to the following conditions: * * The above copyright notice and this permission notice shall be included in all copies or * substantial portions of the Software. * * Use of the Software is limited solely to applications: (a) running on a Xilinx device, or * (b) that interact with a Xilinx device through a bus or interconnect. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING * BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND * NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN * CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. * * Except as contained in this notice, the name of the Xilinx shall not be used in advertising or * otherwise to promote the sale, use or other dealings in this Software without prior written * authorization from # Xilinx. |

## 5 Archiving of Compliance Artifacts

It is important to manually audit all components used in Project to check the licenses and identify the license decisions in Fossology. It is important that the results of the audit should be stored in a form that is tool independent, readable, and understandable to all stake holders involved. In Fossology, 'bill of materials' could be generated for each source code package uploaded and audited. The bill of materials may be generated in different formats like SPDX RDF, SPDX tag:value, and doc. In the Project, the bill of materials are generated in SPDX RDF format, for each source code package, and stored in our repositories.

## 6 Consolidation of results of audit work

The results from audit of various source packages are consolidated in an excel sheet, that acts as a repository. The respository could be used to retrieve details of audit of a individual source packages using filters. This helps in retrieving audit information without going through individual license clearing reports. The excel sheet would be stored in internal repositories of the Project.

## 7 Remediation of non-compliant Intellectual Property related findings

If there are any non-compliant intellectual property related findings in the audit of the source code, or if license non-compliances are found out by any internal stakeholders, including developers/testers/documentation, issues should be created for each finding in the private gitlab repository, Private SBOM issues, that is maintained by the IP-compliance team.

The IP-compliance team discuss the non-compliant IP finding within the team, and if needed, involve the respective developement team who works with the components in question. If the non-compliant situation could be rectified by an action by the upstream open source project, the audit team may raise the issues upstream.

If that is time consuming or not feasible, the team may look for options to remove the file where the non-compliant finding was found, or upgrade the component with a newer version where the issue does not exist, or replace the component with another component.

The status of the issue may be updated at Private SBOM issues, and when a decision is made on the resolution and subsequent action is taken, the issue should be closed.