

Zephyr Project: Results from Applying Open Source Best Practices in Embedded

Kate Stewart, VP Dependable Embedded Systems

#OSSummit @ kate stewart

Zephyr Project



- **Open source** real time operating system
- **Developer friendly** with vibrant community participation
- Built with **safety and security** in mind
- Broad SoC, board and sensor support.
- Vendor Neutral governance
- Permissively licensed Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**
- Product development ready using LTS includes security updates
- Certification ready with Zephyr Auditable_

THELINUX FOUNDATION PROJECTS

Open Source, RTOS, Connected, Embedded Fits where Linux is too big





| Operating System | First Commit | Controls Commits | Declared License | Total Contributors | Contributors in last month | Total Commits | Commits in last month |
|---------------------|-----------------|----------------------|--|-----------------------|----------------------------|------------------|-----------------------|
| Zephyr | 2014/11 | community | Apache-2.0 | 1863 | 269 | 88,107 | 1,777 |
| nuttX | 2007/? | community | BSD-variant \rightarrow Apache-2.0 | 492 | 49 | 51,863 | 248 |
| RT-Thread | 2009/06 | community | $\text{GPL-2.0} \rightarrow \text{Apache-2.0}$ | 661 | 30 | 15,524 | 77 |
| RIOT | 2010/09 | community | LGPL-2.1 | 342 | 17 | 44,624 | 137 |
| Tizen RT | 2015/04 | Samsung | BSD-variant \rightarrow Apache-2.0 | 183 | 14 | 10,796 | 41 |
| FreeRTOS | 2004/07 | Richard Barry | GPL-2.0 w/ FreeRTOS \rightarrow MIT | 146 | 12 | 3,320 | 38 |
| SeL4 | 2014/07 | community | GPLv2 AND BSD-2-Clause | 100 | 8 | 4,423 | 27 |
| Contiki-NG | 2017/10 | community | BSD-3-Clause | 217 | 6 | 17,656 | 35 |
| myNewt | 2015/06 | community | Apache-2.0 | 134 | 4 | 10,785 | 6 |
| ThreadX | 2020/05 | $MSFT \to community$ | $MSL\toMIT$ | 15 | 4 | 148 | 12 |
| mbed OS | 2013/02 | ARM | Apache-2.0 or BSD-3-Clause | 691 | 2 | 34,558 | 2 |

Data extracted on 2023-12-01 from github

https://github.com/zephyrproject-rtos/zephyr Total commits: 85,565 D zephyrproject-rtos / zephyr Public ♀ Fork 5.3k ☆ Star 8.5k Total contributors: 1,800 ssues 1.7k 🏥 Pull requests 707 💭 Discussions 🕑 Actions 🕀 Projects 17 🖽 Wiki 🕐 Security 58 ~ Insights About https://github.com/zephyrproject-rtos/zephyr/pulse/month 12 main - 12 106 branches 5 181 tags Go to file Code -Primary Git Repository for the Zephyr Monthly contributors: 216 evgeniv-paltsev and ihedberg doc: release-notes: arc: reword VPX part 6076d54 1 hour ago 35,565 commits Project, Zephyr is a new generation. scalable, optimized, secure RTOS for .github github: security: Fix supported versions vesterday multiple hardware architectures. Monthly commits: 1,473→ 2 commits/hour arch llext: Cleanups noted in initial PR 3 weeks ago docs.zephyrproject.org boards doc: boards: Set proper languages for syntax highlighting 20 hours ago real-time cmake cmake: extensions: Check status of "zephyr,memory-region" DT nod... last week zephyro doc: release-notes: arc: reword VPX part 1 hour ago embedded-c zephyr-rtos driv drivers: leee802154; cc13xx_cc26xx_subg: buflen sanity check 2 days ago CI Readme dts dts: x86: Remove old atom.dts last week September 18, 2023 - October 18, 2023 Apache-2.0 license Period: 1 month include/zenhy doc: kernel: k_busy_wait behavior with SYSTEM_CLOCK_SLOPPY_ID... Code of conduct 20 hours ago 4 Security policy nel: init: Build constant in early random generator last week kernel Activity Overview lib posix ensi that pooled inc type is user-configurable last week ☆ 8.5k stars misc misc: generated: upd nfigs.c template with <zephyr/...> prefix last year 376 watching ¥ 5.3k forks modules modules: hal_nordic: cmake: Fix king if uicr DT node is accessible last week 1,129 Active pull requests 402 Active issues Report repository doc: samples: smbus: Add console highlig 15 hours ago samples scripts twister: Fix description of relationship between filter an 2 days ago Releases 114 ₽ 772 11 357 277 · 125 share sysbuild: Support SB CONF FILE and SB EXTRA CONF FILE a last week Merged pull requests Open pull requests Closed issues New issues C Zephyr 3.4.0 (Latest) snippets snippets: xen_dom0: add support for Renesas R-Car Gen3 boards on Jun 16 SOC linker; esp32; move snippets-section within rom boundary last wee 113 releases submanifests submanifests: optional: update CHRE revision 2 days ago Excluding merges, 216 authors have pushed 1,438 commits subeve 18 hours ago Contributors 1,800 fs: fix missing semicolon in fuse_fs_access.c to main and 1,473 commits to all branches. On main, 3,376 tests tests: Update sys_kernel benchmark 2 days ag files have changed and there have been 119.637 additions Checkpatch.conf checkpatch: Remove ext/ from excludes last yea and 23,288 deletions .clang-format clang-format: flag * SECTION FOREACH as for loop 5 months ago 0 + 1,789 contributors

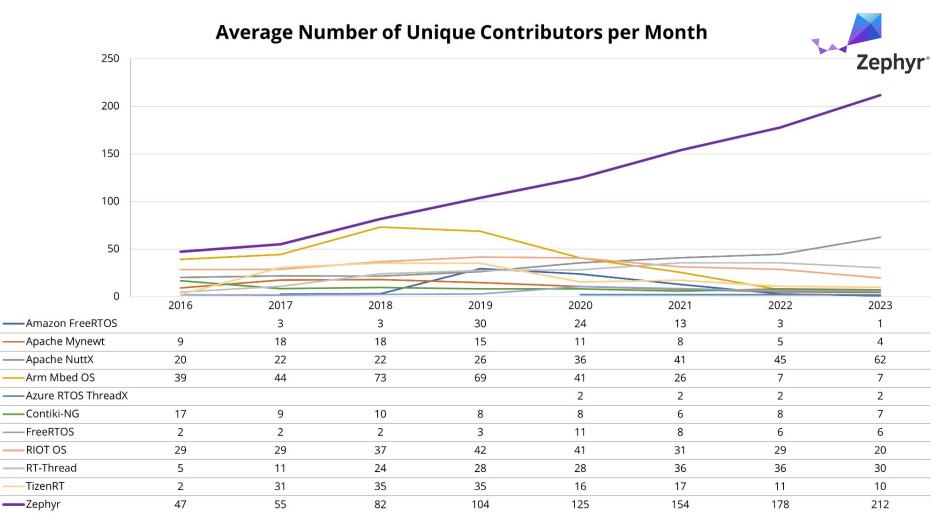
Codecov.vml

vamilint: fix all vamilint comments errors

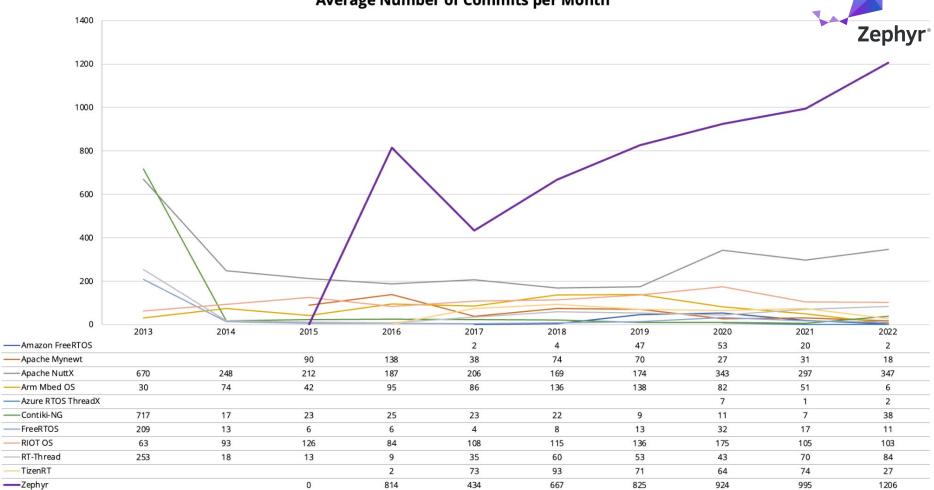
10 months ago

Methodology - with data extracted 2023-10-19 Zephyr

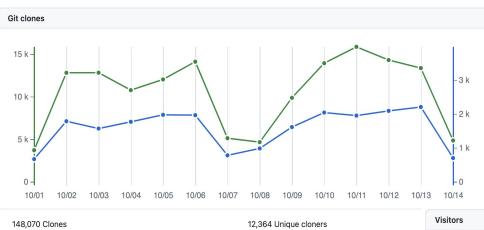
| | | | | | | | | Zephyr® |
|---------------------|-----------------|----------------------|--|---------------------|-----|----------------------------|------------------|--------------------------|
| Operating System | First Commit | Controls Commits | Declared License | Total Contribute | | Contributors in last month | Total Commits | Commits in last month |
| Zephyr | 2014/11 | community | Apache-2.0 | 1 | 863 | 269 | 88,107 | 1,777 |
| nuttX | 2007/? | community | BSD-variant \rightarrow Apache-2.0 | | 492 | 49 | 51,863 | 248 |
| RT-Thread | 2009/06 | community | $\text{GPL-2.0} \rightarrow \text{Apache-2.0}$ | | 661 | 30 | | 77 |
| RIOT | 2010/09 | community | LGPL-2.1 | | | •, | /1 | 137 |
| Tizen RT | 2015/04 | Samsung | BSD-variant \rightarrow Apache-2.0 | 2. | 45 | commit | s/hou | ۲ ₄₁ |
| FreeRTOS | 2004/07 | Richard Barry | GPL-2.0 w/ FreeRTOS \rightarrow MIT | | | | | 38 |
| SeL4 | 2014/07 | community | GPLv2 AND BSD-2-Clause | | 100 | 8 | 4,423 | 27 |
| Contiki-NG | 2017/10 | community | BSD-3-Clause | | 217 | 6 | 17,656 | 35 |
| myNewt | 2015/06 | community | Apache-2.0 | | 134 | 4 | 10,785 | 6 |
| ThreadX | 2020/05 | $MSFT \to community$ | $MSL\toMIT$ | | 15 | 4 | 148 | 12 |
| mbed OS | 2013/02 | ARM | Apache-2.0 or BSD-3-Clause | | 691 | 2 | 34,558 | 2 |



Average Number of Commits per Month

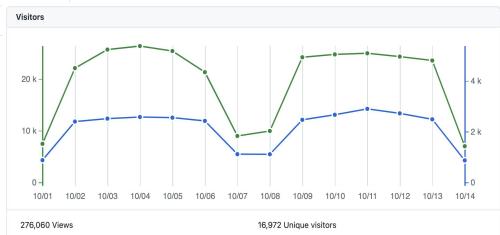






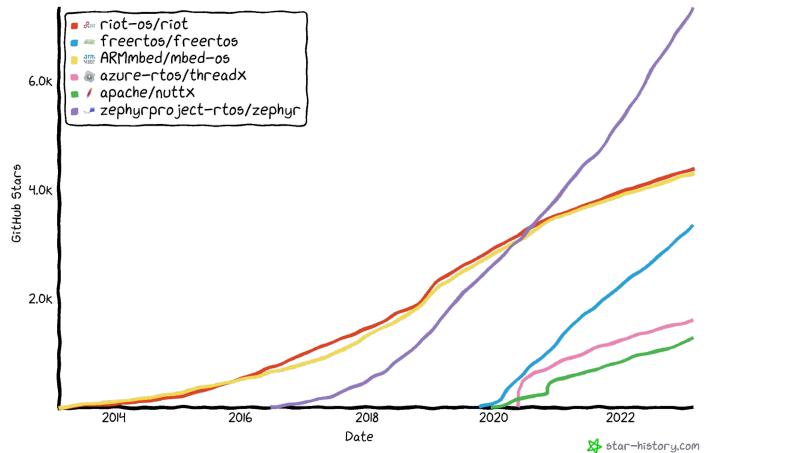
2023-10-01 → 2023-10-14

~883 unique clones per day ~1212 unique visitors per day

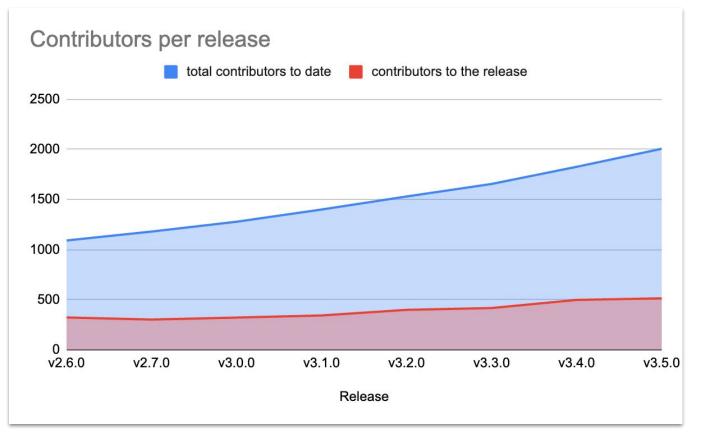


Github Stars History





Contributors Growth per Release

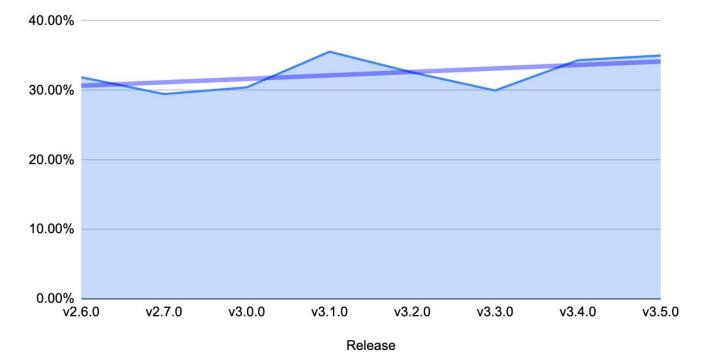


Zephyr

New Contributors per Release



% of first-time contributors

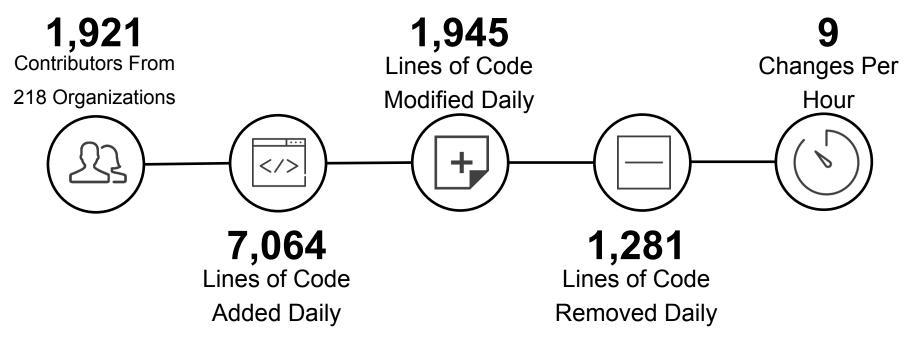


How does this compare to the Linux Kernel?



How does this compare to Linux?

6.5 Linux Kernel Statistics*



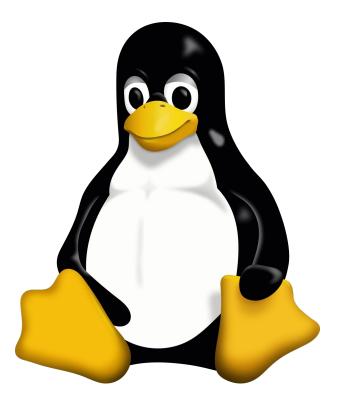
* Source: <u>https://lwn.net/Articles/948970/</u> Time period for 6.5: 2023/6/26-2023/8/27=63 days Also data from: Source: <u>https://github.com/gregkh/kernel-history/blob/master/kernel_stats.ods</u>



So what was it like when Linux started?

UNIX Source Available: SVR4, MINIX 1.5, 4.3BSD

Commercial Distributions: A/UX, IBM AIX, Dec Ultrix, HP-UX, IRIX, SunOS, MIPS RISC/os, Xenix ...





#ossummit

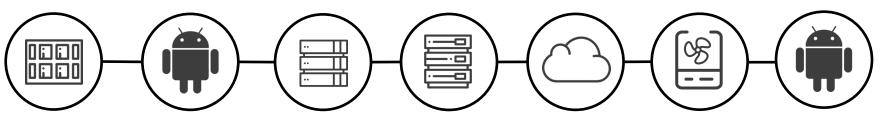
100%

Supercomputer Market 82% Smartphone Market Share **2nd** To Windows in Enterprise **90% 90%** Mainframe Public Clou

Mainframe Public Cloud Customers Workload 69%

#1

Embedded Internet Systems Market Client



Every market Linux has entered it eventually dominates



#ossummit

Lessons Learned by Linux Community circa 2016/2017

Linux Kernel Development Report

Jonathan Corbet, *LWN.net* Greg Kroah-Hartman, *The Linux Foundation*

Source:

https://www.linuxfoundation.org/tools/sta te-of-linux-kernel-development-2017/

More recent stats can be found at: <u>https://www.linuxfoundation.org/tools/lin</u> <u>ux-kernel-history-report-2020/</u>

- Short release cycles are important.
- Process scalability requires a distributed, hierarchical development model.
- Tools matter.
- The kernel's strongly consensus-oriented model is important.
- A related factor is the kernel's strong "no regressions" rule.
- Corporate participation in the process is crucial.
- There should be no internal boundaries within the project



++ Lessons Learned

- Vendor-neutral environment for technical decision making
- Mix of companies and individuals participating "scratching their itches"
- Streamline upstreaming process DCO "signed-off-by:"
- Public code reviews "reviewed-by:"
- Consensus-oriented decision model email, in-person summits
- Hierarchical development model (maintainer model) "signed-off-by"
- No internal boundaries developer can contribute anywhere
- **Tools matter** git enabled distributed version control push/pull
- Short predictable release cycles and with fixed merge windows
- Stable & LTS: stable and long term support releases support product development
- **KEY:** Developer frustration with status quo inspires creative solutions.



So what lessons did **Zephyr apply from the** Linux Kernel **Community?**





Zephyr's Vision

The Zephyr Project strives to deliver the **best-in-class RTOS** for connected resource-constrained devices, built to be secure and safe.

Zephyr Developers Decide Technical Directions

- Configuration: kconfig & kbuild added in 2015 prior to launch
- Unified kernel: nano + microkernels \rightarrow unified kernel in 2016
- Infrastructure: Gerrit/JIRA \rightarrow GitHub/Issues in 2017
- **Build system:** kbuild \rightarrow **cmake** in 2018
- Other areas:
 - APIs & HALs reworked
 - Modularization & Device Tree support
 - Release & LTS processes refined

Applying ++ Lessons Learned

| Linux Best Practice | Zephyr Adoption |
|--|---|
| Vendor Neutral Decision Making | Yes, Project support from multiple companies. |
| Companies and Individuals Participate | Yes, TSC has companies & community participation. |
| Streamline upstreaming process | Yes, see / <u>CONTRIBUTING.rst</u> , DCO used |
| Public code reviews? | Yes, issues & pull requests reviewed on https://github.com/zephyrproject-rtos/zephyr |
| Consensus Oriented Decision Models | Yes, TSC votes on features & release readiness. |
| Hierarchical development (Maintainers) | Yes, see /MAINTAINERS.yml |
| No Internal Boundaries | Yes, anyone can make pull request for any area |
| Distributed version control | Yes, see /CONTRIBUTING.rst |
| Short Release Cycle (w/ Merge Window) | Yes, 10 week merge, 2-4 week stabilize |
| Long Term Support Releases | Yes, LTS 1 had 4 update release, LTS 2 active maintain |



#ossummit

So what does Zephyr support today?











Cortex-M, Cortex-R & Cortex-A



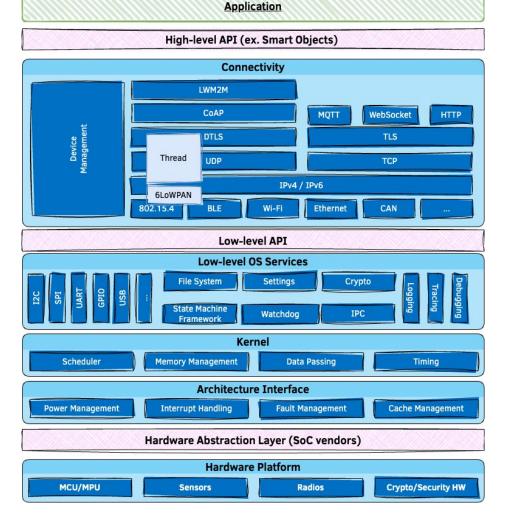
x86 & x86_64



docs.zephyrproject.org/latest/hardware/index.html#hardware-support



Architecture

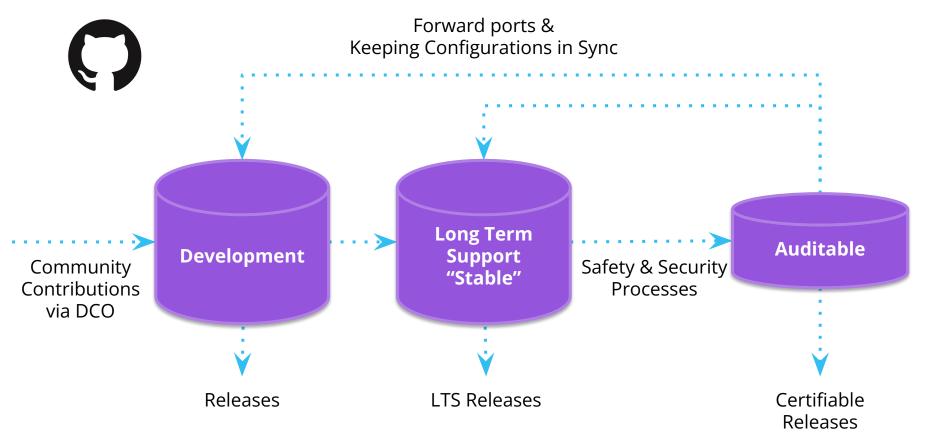


What about Zephyr security?



Code Repositories







Long Term Support (Zephyr 2.7.x)

- Product Focused
- Current with latest **Security Updates**
- Compatible with new hardware
 Functional support for new hardware is regularly backported
- **Tested**: Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- <u>Supported for 2+ years</u>
- **1** Doesn't include cutting-edge functionality

Long Term Support (LTS - 1.14)



| Code () Issues 8 | 96 🕅 Pull requests 431 O Actions 📰 Projects 9 🔠 WH4 🕕 Security 📓 | Insights | | Code 🕦 Issues | 1,818 🗋 Pull requests 488 O Actions 📜 Projects 10 📰 Wiki 🕕 Secu | rity 0 🔤 Ins | |
|------------------|--|-----------------|---|--|---|---|--|
| C zephyn-v1.14.0 | Zephyr 1.14.0 all adda release the on Apr 16 - 51% commits to master since the release We are besad to amounce the release include: Major enhancements with this release include: - The Zeybyr protect now support sow r160 different board configurations | Code Issues | 6 / zephyr O'Unweten + 319 868 D Pull requests 438 O Actions E Projects 9 WW O'Security Lin | asc release | Zephyr LTS 1.14.2 (Mainternance Re realist released this 25 days ago - 11280 commits to master since this release This is an LTS maintenance release with fixes. Security Vulnerability Related | Code O issues 12 | /zephy Pute: © Unwach 380 ¥ formed 83 \$ stand \$ stand< |
| | spanning & architectures. All architectures are reprovuly tested and validated using one of the many smitulision platforms supported by the project: CBMU, Renote, ARC Simulator, and the native POSIX configures and the second second second and validamental quarkity attractional second second and validamental quarkity attraction of the second second and validamental quarkity attraction of the second second and validamental quarkity attraction of a new CPU attraction ball size by hundrades of bytes. TICKLESS, KEINEL mode is now the default on all architectures. TICKLESS, KEINEL mode is now the default on all architectures with the adational of a new CPU attractive planet continues to evolve with the adation of a new CPU attractive planet behavior. API (which on uniprocessor systems reduces to the same code). 2 Zephyr now has support for the 48, 64 architecture. It is currently implemented only for GBMU targets, support strategies on so. 2 We ve overhauled the Network packet ner-plat API and moves distribu- tion days. | Careford A.1.1. | Reading reader this 28 days ago - 5128 committe to master since this release This is an LTS maintenance release with fixes, as well as Bluetooth qualification listings for the Bluetooth protocol stack included in Zephyr. | | Operating Value Product The following security vulnerabilities (CVEs) were addressed in this release: CVE-2020-1001 CVE-2020-10021 CVE-2020-10021 CVE-2020-10022 CVE-2020-10023 CVE-2020-10024 CVE-2020-10024 | 23 days ago nashif ○ v1.14.3 @ ○ r1277385 Compare • | Zephyr v1.14.3 (unit) This is an LTS maintenance release with fixes. Security Vulnerability Related The totowns security vulnerabilities (CVES) were addressed in this |
| | | | | OVE-2020-10027 OVE-2020-10027 OVE-2020-10028 More detailed information can be found in: https://docs.zephyproject.org/latest/security/vulnerabilities.html Issues Fixed These GilHub issues were addressed since the previous 1.14.0 tagged release: | | release: | |
| | | | Outilification: 1.14.x Host subsystem qualified with QDID 138258 1.14.x Most subsystem qualified with QDID 138259 1.14.x Controller component qualified on Nordic nIF52 with QDID 138 Issues Fixed | 5679 | | | These BiH-Ju issues were addressed since the previous 114.0 tagged release. #18334 - DNS resolution is broken for some addresses in master/2-0-pre #19979 - Bluetoch: Controller Missing LL_ENC_RSP after HOLTX Negative Reply #21107 - LL_ESSET1 and 'mproceile add to bue ren' in LL Controller #21275 - testsheltmet, ptk tailad on mimort050_exh based. |

Delivered bug fixes and latest security updates for 2 years!

Auditable



- An **auditable code base** will be established from a **subset** of the Zephyr OS LTS
- Code bases will be kept in sync
- More rigorous processes (necessary for certification) will be applied to the auditable code base.
- Processes to achieve selected certification to be:
 - Determined by Safety Committee and Security Committee
 - Coordinated with Technical Steering Committee

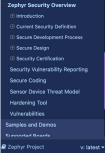


Project Security Documentation



- Project Security Overview
- Started with documents from other projects
- Built around Secure
 Development, Secure Design, and Security Certification
- Ongoing process, rather than something to just be accomplished





Docs / Latest » Security » Zephyr Security Overview Open on GitHub

This is the documentation for the latest (main) development branch of Zephyr. If you are looking for the documentation of previous releases, use the drop-down menu on the left and select the desired version.

Zephyr Security Overview

Introduction

This document outlines the steps of the Zephyr Security Subcommittee towards a defined security process that helps developers build more secure software while addressing security compliance requirements. It presents the key ideas of the security process and outlines which documents need to be created. After the process is implemented and all supporting documents are created, this document is a top-level overview and entry point.

Overview and Scope

We begin with an overview of the Zephyr development process, which mainly focuses on security functionality.

In subsequent sections, the individual parts of the process are treated in detail. As depicted in Figure 1, these main steps are:

- Secure Development: Defines the system architecture and development process that ensures adherence to relevant coding principles and quality assurance procedures.
- 2. Secure Design: Defines security procedures and implement measures to enforce them. A security architecture of the system and relevant sub-modules is created, threats are identified, and countermeasures designed. Their correct implementation and the validity of the threat models are checked by code reviews. Finally, a process shall be defined for reporting, classifying, and mitigating security issues..
- Security Certification: Defines the certifiable part of the Zephyr RTOS. This
 includes an evaluation target, its assets, and how these assets are protected.
 Certification claims shall be determined and backed with appropriate evidence.



Software Supply Chain Support



- Zephyr ships an **SBOM** (Software Bill of Materials) with each release
- Downstream consumers can leverage built-in tools to, in turn, generate source & build SBOMs for their deliverables

```
[...]
FileName: ./zephyr/zephyr.elf
SPDXID: SPDXRef-File-zephyr.elf
FileChecksum: SHA1: e74cebcac51dabd799957ac51e4edcd32541103d
[...]
Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM SPDXRef-File-dev-handles.c
Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM SPDXRef-File-isr-tables.c
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libapp.a
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libzephyr.a
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libisr-tables.a
```

CVE Numbering Authority



<u>Registered with MITRE</u>

in 2017

- We issue our own CVEs
- Zephyr Project Security Incident Response Team (PSIRT)
 - Volunteers from the Security
 Subcommittee led by the Zephyr
 Security Architect.

Zephyr Project

The majority of the links on this page redirect to external websites E; these links will open a new window or tab depending on the web browser used.

| Scope | Zephyr project components, and vulnerabilities that are not in another CNA's scope |
|------------------------|--|
| Root | MITRE Corporation |
| Security Advisories | View Advisories |
| Program Role | CNA |
| Organization Type | Vendors and Projects |
| Country* | USA |

OpenSSF Gold Badge

- <u>Core Infrastructure Initiative</u> Best Practices Program
- Awards badges based on "project commitment to security"
- Mostly about project infrastructure: is project hosting, etc following security practices
- Gold status since Feb, 2019



Zephyr Project

xpand panels Show all details Hide met & N/A

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved an Open Source Security Foundation (OpenSSF) best practices badge. Show details

If this is your project, please show your badge status on your project page! The badge status looks like this: openssf best practices gold Here is how to embed it: Show details

These are the passing level criteria. You can also view the silver or gold level criteria.

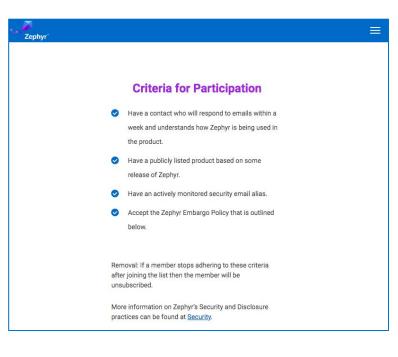
| ✓ Basics | 13/13 • |
|------------------|---------|
| ✓ Change Control | 9/9 • |
| ✓ Reporting | 8/8 • |
| ✓ Quality | 13/13 • |
| ✓ Security | 16/16 • |
| ✓ Analysis | 8/8 • |



Vulnerability Alert Registry



- For an embargo to be effective, product makers need to be notified early so they can remediate
- <u>Goal</u>: Zephyr to fix issues within 30 days to give vendors 60 days before publication of vulnerability
- Product makers can register to receive these alerts for free by signing up at Vulnerability Alert Registry



Zephyr PSIRT: Remediation and Response

Advisory Issued by project on 20201208:

- Zephyr current release (2.4) does not use Fnet or other Ο stacks.
- The Zephyr LTS release 1.14 contains an 0 implementation of the TCP stack from Fnet.

Of the vulnerabilities reported in Fnet, 2, <u>CVE-2020-17468</u>, and CVE-2020-17469, are in the IPv6 Fnet code, one, CVE-2020-17467, affects Link-local Multicast Name Resolution LLMNR), and 2, CVE-2020-24383, and CVE-2020-17470 affect DNS functionality.

None of the affected code has been used in the Zephyr project, while 1.14 does use the Fnet TCP, it does not use the affected IPv6, DNS or LLMNR code. zephyrproject.org/zephyr-security-update-on-amnesia33

oria an initiativ that aims at providing the community with the largest study on the security of TCP/IP stacks. Project Memoria's goal is to develop the understanding of common bugs behind the vulnerabilities in TCP/IP stacks, identifying the threats they nose to the extended enterprise and how to mitigate those

Research Report Executive Summary

<) FORESCOUT

AMNESIA:33

AMNESIA:33 is the first study we have published under Project Memoria In this study, we discuss the results of the security analysis of seven open source TCP/IP stacks and report a bundle of 33 new vulnerabilities found in four of the seven analyzed stacks that are used by major IoT, OT and IT device vendors

Four of the vulnerabilities in AMNESIA:33 are critical, with potential for remote code execution on certain devices. Exploiting these vulnerabilities. could allow an attacker to take control of a device, thus using it as an entry point on a network for internet-connected devices, as a pivot point for lateral movement, as a persistence point on the target network or as the final target of an attack. For enterprise organizations, this means they are at increased risk of having their network compromised or having malicious actors undermine their business continuity. For consumers, this means that their IoT devices may be used as part of large attack compaigns, such as botnets, without them being aware





tol free 1-866-377-8771

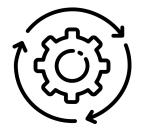


AMNESIA:33 | EXECUTIVE SUMMARY

Zephyr Security Summary









Documented secure coding practices

Vulnerability response criteria publicly documented Weekly Coverity scans MISRA scans SBOM generation

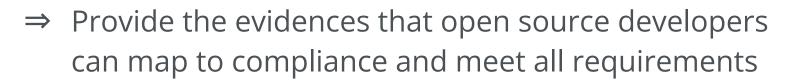
What's all this about Zephyr safety?



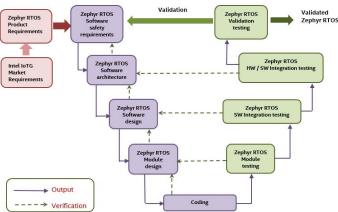
Compliant Development: V-model



- It is difficult to map a stereotypical open-source development to the V-model
- Specification of features
- Comprehensive documentation 0
- Traceability from requirements to source code
- Number of committers and information known about them







Safety Collateral Proposal



| Artifacts | Type of Doc | Owner | Work in progress Visibility |
|---|--------------|-------------------------|--------------------------------|
| Plans | Category | | |
| Safety Development Plan | Plan/Process | Safety Committee | Public - Project Docs |
| Safety Assesment Plan | Plan/Process | FSM | Safety Committee Github |
| Verification / Validation / Integration Test Plan | Plan/Process | Testing WG | Public - Project Docs |
| Software Development Plan | Plan/Process | TSC | Public - Project Docs |
| Configuration and Change Management Plan | Plan/Process | TSC | Public - Project Docs |
| Coding Guideline | Plan/Process | TSC | Public - Project Docs |
| Tools Documentation | Plan/Process | TSC | Public - Project Docs |
| Specifications | Category | | |
| Safety Scope Definition | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Requirement Specification (SRS) ** | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Architecture and Interface Specification (SAIS) ** | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Component Design Specification (SMDS) ** | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Component Test Specification (SMTS) ** | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Integration Test Specification (SITS) ** | Spec. | Safety Committee | Safety Committee Github |
| Safety Software Test Specification (STS) ** | Spec. | Safety Committee | Safety Committee Github |
| | | Salety Committee | Salety Committee Github |
| Sources | Category | | |
| Source Code | Source | TSC | Public |
| - Coding Guideline Compliance | Source | TSC | Public |
| Project Documentaton | Source | TSC | Public |
| Software Requirement Specifications | Spec | TSC | Public |
| Software Architecture and Interface Specification | Spec | TSC | Public |
| Software Component Design Specification | Spec | TSC | Public |
| Project Testing | Source | TSC | Public |
| Software Component/Unit Test Specification | Spec | TSC | Public |
| Software Integration Test Specification | Spec | TSC | Public |
| - Software Test Specification | Spec | TSC | Public |
| - Tests | Source | TSC | Public |
| Reports | Category | | |
| Code Review Report (pre-merge) | Report | TSC | Public |
| Code Change Test Report (post-merge) | Report | Testing WG | Public |
| Test Coverage Report | Report | Testing WG | Public |
| Coding Guideline Compliance Report | Report | Safety WG & Security WG | Public |
| Traceability Report | Report | Safety WG | Public |
| Tools Classification | Report | Safety Committee | Public |
| Tools Validation | Report | Safety Committee | TBD (based on specific tools) |
| Fault Injection Test Report | Report | Safety Committee | Safety Committee |
| Safety Traceability Report (for Safety Scope) ** | Report | Safety Committee/FSM | Safety Committee |
| Safety Test Coverage Report (for Safety Scope) ** | Report | Safety Committee/FSM | Safety Committee |
| Safety Analysis (e.g., FMEA) | Report | FSM | Safety Committee |
| Manuals | Category | | |
| Software User Manual | Manual | TSC | Public |
| Safety Manual | Manual | FSM | Safety Committee |
| Certificates | manaa | | carety committee |
| All safety certificates | Certificate | Safety Committee | N/A |

- Requirement definition, Source Code & Test linkage are public; and developed in open using <u>strictdoc</u>
- The set of requirements (and associated traceability) are applicable to safety scope is managed by the safety committee.
- Other project artifacts have owners descignated.

Initial certification focus



- Start with a limited scope of kernel and interfaces
- Initial target is IEC 61508 SIL 3 / SC 3 (IEC 61508-3, 7.4.2.12, Route 3s)
- Option for 26262 certification has been included in contract with certification authority should there be sufficient member interest

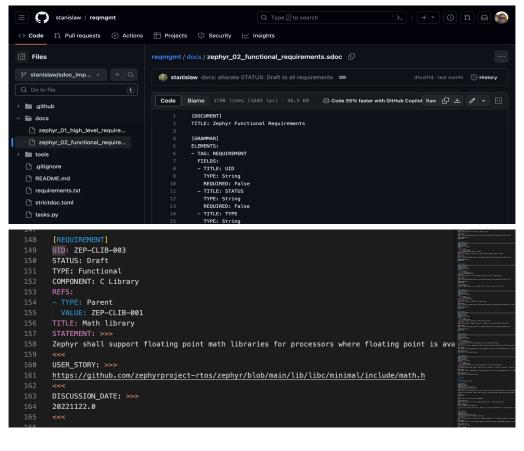
| | | | Zephyr RTO5 | | |
|---|------------------------|--------------------------------|--------------------------|--------------------------------------|-----------------------------------|
| Zephyr | Public Kernel API | | Low Level API fe | Device Model / Devic Driver Model | |
| nel Services / Schoduling, interrupt | s, and Synchronization | , | | Ĩ. | OS Services |
| Threads | Scheduling | Interrupts | Semaphores | Condition Variables | |
| System Threads | Workqueue | Poling API (Event Poling) | Mutexes / Fulex | Symmetric Multiprocessing | Logging / Debug |
| Data passing | | | |] | properties) |
| Queues | LIFOS | Message Queues | Pipes | | Architecture Interfac |
| FIFOs | Stacks | Malboxes | | | Power Managment |
| Diming | Memory Managemen | Miscellanous | (Other services) | 1 | Interrupt Handling |
| Kernel Timing | Memory Heaps | CPU idlin | ig Floating ; service | | Common Architecture Interfaces |
| Timers | Memory Slaps | Atomic servi | cces Versio | n Thread local storages | MMU/MPU |

Scope can be **extended** to include **additional components** with associated **requirements** and **traceability** as determined by the safety committee

Current requirements work

Zephyr

- Used tooling: StrictDoc (<u>https://github.com/strictdo</u> <u>c-project/strictdoc</u>)
- Decision on UIDs for requirements (UID will be generated by StrictDoc)
- Hierarchical structure of requirements that works for the project
- Capturing the requirements in StrictDoc



What's happening now..

Safety Committee

- Safety Certification Strategy decisions
 - Scope of certification
 - Certification standards
 - Certification timeline
- Assessment and audit specific tasks
- Owner of certification artefacts
- Participation limited to the project's platinum members, the safety architect and the functional safety manager

Safety Working Group

- Enabling safety qualifications/ certifications in the project
- Working on creating the required documentation and evidences
 - Setting up requirements management tooling
 - creating/deriving and documenting requirements
- Open to everyone to participate, join today: <u>https://lists.zephyrproject.org/g/safety-wg</u>

Results of applying the best practices



Zephyr in the wild... 5.4K Forks!



About

Primary Git Repository for the Zephyr Project. Zephyr is a new generation, scalable, optimized, secure RTOS for multiple hardware architectures.

docs.zephyrproject.org

| io | t real-time microcontroller | | | | | | | |
|--------------|--------------------------------|--|--|--|--|--|--|--|
| er | nbedded bluetooth bluetooth-le | | | | | | | |
| m | cu rtos zephyr zephyros | | | | | | | |
| er | nbedded-c zephyr-rtos | | | | | | | |
| | Readme | | | | | | | |
| ٥ <u>t</u> ə | Apache-2.0 license | | | | | | | |
| 69 | Code of conduct | | | | | | | |
| ٥ <u>t</u> a | Security policy | | | | | | | |
| -^- | Activity | | | | | | | |
| ☆ | 8.8k stars | | | | | | | |
| \odot | 378 watching | | | | | | | |
| ಳ | 5.4k forks | | | | | | | |

Source:

https://github.com/zephyrproject-rtos/zephyr



HOME PROGRAM PRODUCTS Y PARTNERS CONTACT DEVELOPER AREA YQ

Pulga Core V2.0

The Caninos Loucos Pulga board is a powerful microcontroller with a large number of sensors, highly secure, and ideal for IoT applications. Completely designed in Brazil.

CANINOS LOUCOS

The low power board is approximately the size of a quarter dollar coin (24,26mm) and supports Bluetooth 5.0, allowing for wireless connection between multiple Pulgas.

Aspects such as modularity, via an autonomous core board and an optional base board, and energy harvesting capability, enables great exibility for hardware interfaces prototyping.

The base board allows for adding functionality for custom applications. For example, by adding long distance wireless protocols and new sensors, you can meet the demands of dierent projects.

Finally, the harvesting allows for capturing energy from dierent environmental sources, ensuring energetic autonomy to the board.

Website:: <u>https://caninosloucos.org/en/pulgacore-v2-en/</u> Code: <u>https://github.com/caninos-loucos/pulga-zephyr</u>

Technological Integrated Systems Laboratory (LSI-TEC) with the support of the Polytechnic School of the University of São Paulo (Poli-USP)



ENGLISH 🔤

Products Running Zephyr Today







Proglove

Ruuvi Tag



PHYTEC Distancer



Keeb.io BDN9



Hati-ACE

Oticon More



Adhoc Smart Waste



GNARBOX 2.0 SSD



Anicare Reindeer Tracker



Safety Pod



BLiXT solid state circuit breaker



Moto Watch 100



tracker

Runava

Rigado IoT Gateway



Livestock Tracker



Laird Connectivity sensors & gateways

zephyrproject.org/products-running-zephyr



BeST pump monitoring



Vestas Wind Turbines









Arduino Portenta H7

ESP32



Sipeed HiFive1



nRF9160 DK



STM32F746G Disco



M5StickC PLUS



TDK RoboKit 1



BBC microbit v2



Blue Wireless Swan



Arduino Nano 33 BLE



Intel UP Squared



Dragino LSN50 LoRA Sensor Node



Microchip SAM E54 Xplained Pro Evaluation Kit



Raspberry Pi Pico



Altera MAX10



NXP i.MX8MP EVK



Adafruit Feather M0 LoRa



u-blox EVK-NINA-B3





170+ Sensors Already Integrated

amg88xx









sm351lt th02 ti_hdc ti hdc20xx tmp108 tmp116 v15310x wsen_itds

Zephyr°

github.com/zephyrproject-rtos/zephyr/tree/main/drivers/sensor

IoT Connectivity Options

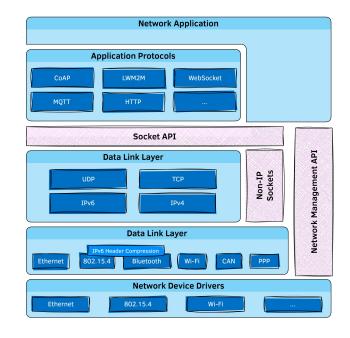


- Wide variety of **communication protocols**
 - Ethernet, 802.15.4, Thread, LoRa, Bluetooth, CAN bus, ...
- **Core network protocols** like IPv6, IPv4, UDP, TCP, ICMPv4, and ICMPv6.
- **Security** (ex. TLS, DTLS, ...)
- **Cloud integration** using MQTT, CoAP and HTTP protocols
- Over-the-air updates
- **Device management** using OMA LwM2M 1.1 protocol

Native IP Stack

- Built from scratch, on top of Zephyr native kernel concepts
- Dual mode **IPv4/IPv6 stack**
 - DHCP v4, IPv4 autoconf, IPv6 SLAAC, DNS, SNTP
- Multiple network interfaces support
- Time Sensitive Networking support
- BSD Sockets-based API
- Supports IP offloading
- Compliance and security tested





Bluetooth Host and Mesh



- Bluetooth 5.3 compliant
- Highly configurable
- Portable to all architectures supported by Zephyr
- Low Energy & experimental Bluetooth Classic
- IPSP/6LoWPAN for IPv6 connectivity over Bluetooth LE
- Multiple HCI transports

Bluetooth Low Energy Controller



- **Bluetooth 5.3 compliant** and qualified (5.1)
- Support for multiple BLE radio hardware architectures
 - Nordic nRF5x on Arm Cortex-M
 - VEGAboard on RISC-V
- Proprietary radios (downstream only)
- Unlimited role and connection count
- Concurrent multi-protocol support ready
- Multiple advertiser and scanner instances

Zephyr USB Device Stack



- USB 2.0 & USB-C support
- Supports multiple MCU families (STM32, Kinetis, nRF, SAM,...)
- Supports most common devices classes: CDC, Mass Storage, HID, Bluetooth HCI over USB, DFU, USB Audio, etc.
- Tight integration with the RTOS
- Native execution support for emulated development on Linux
- WebUSB support

Power Management



- Goal: use as little power as possible
- Cross-platform (architecture / SoC agnostic)
- Tickless scheduler
- Handled by the kernel / Customizable by the user

Describe & **configure** the available hardware on the target system **Decouple** the application from the hardware



```
Zephyr
```

```
&i2c1 {
    pinctrl-0 = <&i2c1_scl_pb8 &i2c1_sda_pb9>;
    pinctrl-names = "default";
    clock-frequency = <I2C_BITRATE_FAST>;
    status = "okay";
    lsm6ds1@6a {
        compatible = "st,lsm6dsl";
        reg = <0x06a >;
    };
    hts22105f {
        compatible = "st,hts221";
        reg = <0x5f >;
    };
    // ...
};
```

.dts file example

Devicetree

Secure boot / Device Management



- Leverage **MCUboot** as secure bootloader
- Application binary can be signed/encrypted
 Can use hardware keys
- But also:
 - Downgrade prevention
 - Dependency checks
 - Reset and failure recovery
- Over-the-air (OTA) upgrades
 - OMA LwM2M, Eclipse hawkBit
 - Vendor offerings

Hardware security



- Random Number Generation, ciphering, etc.
- Supported by crypto HW, or SW implementation (TinyCrypt)

• Trusted Firmware integration

- Firmware verification/encryption
- Device attestation
- Management of device secrets





Building on POSIX



- Zephyr apps can run as native Linux applications
 - Easier to debug/profile with native tools
 - Connect to real devices using TCP/IP, Bluetooth, CAN
 - Helps minimize hardware dependencies during the development phase
- Re-use existing code & libraries by accessing Zephyr services through POSIX API
 - Easier for non-embedded programmers
 - Implementation is optimized for constrained systems
 - Supported POSIX subsets: PSE51, PSE52, and BSD sockets

A real-time OS



Benchmark on Arm Cortex-M4F running at 120 MHz

| Operation | Time |
|------------------------|--------|
| Thread create | 2.5 µs |
| Thread start | 3.6 µs |
| Thread suspend | 3.3 µs |
| Thread resume | 3.8 µs |
| Context switch (yield) | 2.2 µs |
| Get semaphore | 0.6 µs |
| Put semaphore | 1.1 µs |

Graphical User Interfaces



- Drivers available for various types of displays
 - LCD
 - OLED
 - Touch panel displays
 - E-ink
- LVGL integration
- Support for video capture and output



© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.

Inter-Process Communication

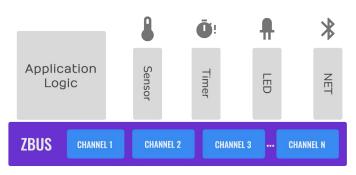
• Built-in kernel services (see table)

• IPC service

- 1-to-1 or 1-to-many communications
- No-copy API
- **zbus** (Zephyr Message Bus)
 - 1-to-1, 1-to-many, or many-to-many channel-based communications
 - Synchronous or asynchronous

| Object | Bidirectional? | Data structure |
|---------------|----------------|----------------|
| FIFO | × | Queue |
| LIFO | × | Queue |
| Stack | × | Array |
| Message queue | × | Ring buffer |
| Mailbox | ~ | Queue |
| Ріре | × | Ring buffer |

Data passing objects available in Zephyr kernel





A typical zbus application architecture

Tracing & Debugging

- Advanced **logging** framework
 - Multiple backends (UART, network, file system, ...)
 - Compile-time & runtime filtering
- **Tracing** framework
 - Visualize the inner-working of the kernel and its various subsystems
 - Object tracking (mutexes, timers, etc.)

| Old Open (1) Open (1) <tho< th=""><th></th><th></th><th></th><th></th><th>Event</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tho<> | | | | | Event | | | | | | | | | | | | | | | | | | |
|--|--------|--------------|-----------|--------|-------|---------|------------|----------|---------|-----------|----------------|-------------|--------|----------|----------|----------|---------|----------|---|----------|-----|---|------|
| 30 01.50 77.11 0 77.11 0 77.11 | | | | | 241 | k Ready | 7200 | 01082200 | 00160, | runs afte | ur 4.3334 ma | 1 (142 cyc) | (00) | | | | | | | | | | |
| 61 0.158 71.1 0 71.1 0 71.1 0 71.1< | | | 514 | 20000 | | | | e 6 | | d and | | | | | | | | | | | | | |
| 201 0.139 0 | | | | | | | | | | | | | | | | | | | | | | | |
| 10 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0 | | | | | | | Runs | tor 4.42 | SU ms (| 145 cycle | (B) | | | | | | | | | | | | |
| 23 01.20 01. | | | | 20000. | 1 135 | | retui | ns after | 229.49 | 21 88. | | | | | | | | | | | | | |
| 33 01.301 01.201 07.21 04.64 7 100 Enti 301 01.201 07.201 04.64 7 100 Enti 301 01.201 04.01 0 | | | | | | | | | | | | | | | | | | | | | | | |
| 11 01-01 01 01 01 01 01 01 01 01 01 01 01 01 0 | | | | | | | 2.0 | | 1 | | | | | | | | | | | | | | |
| 33 01.0 10 10 10 10 10 10 10 10 10 10 10 10 10 | | | | | | | 2005.03 | | | | | | | | | | | | | | | | |
| 30 01.0 10 10 10 10 10 10 10 10 10 10 10 10 10 | | | | | | | | | | | | | | | | | | | | | | | |
| 10 01-01 01 01 01 01 01 01 01 01 01 01 01 01 0 | | | | | | | | | | | | | | | | | | | | | | | |
| 11 01 01 01 01 01 01 01 01 01 01 01 01 0 | | | | Idle 1 | × 100 | Enter | | | | | | | | | | | | | | | | | |
| 34 01.57 11 26 20 35 01.57 11 26 20 30 01.57 11 | | | | Idle | × 188 | Exit | Setu | ns to Id | le | | | | | | | | | | | | | | |
| 237 01.277 11 24 20 41 24 20 51 20 51 20 51 20 51 20 51 20 51 20 51 20 51 20 51 20 5 | | | | | | | NOT CAS | 0 10 | | | | | | | | | | | | | | | |
| 31 01.27 11 52 20 51 01.27 11 52 10 51 01.27 11 | | | | | | | | | | | | | | | | | | | | | | | |
| 33 01.31 01.32 01.52 01 | | | | | | | Retur | ns to Id | le | | | | | | | | | | | | | | |
| 946 0.13 116.07 546 100 | | | | | | | | | | | | | | | | | | | | | | | |
| 511 0.13 512 0.13 7000000000000000000000000000000000000 | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | 22001 | 018cE200 | 001e4, | runs afte | r 30.5 us (| (1 cycles) | | | | | | | | | | | |
| 0 m 000 m 01,553 762 157 000 m 1100 m 1000 m 10000 m 1000 m 10000 m 10000 m 10000 m 1000 m 10000 m 100000 m 10000 m 10000 m 100000000 | 42 | 01.387 145 | 996 1 | Idle i | A 188 | Exit | Retur | ns to Id | le | | | a - 11 - 12 | | | | | | | | | | | |
| 0 m 00156 m 01,503 722 127 0 000 m 1000 m 1000 m 0000 m 00000 m 00000 m 00000 m 000000 | -0150 | Width: 5.0 s | | | | | | | | | | | | | | | | | | | | | |
| | - | | | | -500 | ma | 01.353 | 752 157 | | +500 ms | | +1000 ms | | +1500 ms | | +2000 ma | | +2500 ms | | +3000 ms | | +3500 ms | _ |
| | | | 1 | |] | | 1.1.4 | | | | | 1 1 | | 1 1 | 1 1 | 1.1.0 | 1 1 | | | | | | - |
| | | | | | | | - | | - | - | | | | | | | | | | | | | 44 |
| | | | | 1.1 | | 1 | 1 | | 11 | | | | 1 1 | | | | | 1.11 | | _ | 1 1 | | 11 |
| | | | | | | | | | | | | | | | | | | | | | | | |
| | 121 | 0000084E200 | 000 | | | | | | | | | | | | | | | | | | | _ | |
| | | | | | | | | | | 1 | | | | | | | | | | | | | - |
| | | | | | | 1 | | | | | | | | 1 | | | | | 1 | | | | . L. |
| T2000294E20002 | | | | | | | | | | | - | | | | | | | | | | _ | | |
| | 121 | UUU2000E200 | 0.29 | | | | | | | | | | | | | 1 | | | | | | | |
| | 53 T21 | ococcesHE200 | uus | | | | | | | | | | | | | 1.11 | | | | _ | | | 1 |
| | OR | 2 | | | | | | UI | | | | | | | | | | | | | | | |
| | | | | _ | _ | _ | | | | _ | | | _ | | _ | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | |
| School ar Toxicologie 200000 Toxicologie 20000 Toxicologie 20000 Toxico | T21 | 00028b0E200 | 025 | | | | | - | _ | _ | | | | | | | | _ | _ | | | | |
| | kik | 2 | | | | | | | | | | | | | | | | | | | | | |
| 1200004E2000 | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | Total Run Time | | | | | | | | | | | | |
| | | | | | 26 | 4 Hz | 1.1596 ms | | | | | | | | | | | | | | | (, , , , , , , , , , , , , , , , , , , | (|
| | | @-1 76E | | | 26 | 6 Hz | 6.7138 ms | 0.0305 m | 1 8 | 7890 m | 83.3129 ms | | | | | | | | | | | | |
| | | | | | 0 | 0 Hz | 0.0 ms | | | | 0.0 ms | | | | | | | | | | | | |
| POP POP <td></td> <td></td> <td>@ 0x20003</td> <td>638</td> <td></td> | | | @ 0x20003 | 638 | | | | | | | | | | | | | | | | | | | |
| | 0 | | | | 50 | 10 Hz | 69.8852 ms | 0.0905 n | 1 5 | 18.9514 | 4753.143 | 967.8344 | 98.789 | 6 0.01 | ns 0.00% | 1117.67 | 111.77% | | | | | | |
| POP POP <td>_</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>_</td> <td></td> <td></td> <td></td> <td>0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>_</td> | _ | | | | | | | | _ | | | | 0 | | | | | | | | | | _ |
| No. No. <td>a</td> <td></td> | a | | | | | | | | | | | | | | | | | | | | | | |
| No. No. <td></td> <td>ow started.</td> <td></td> | | ow started. | | | | | | | | | | | | | | | | | | | | | |

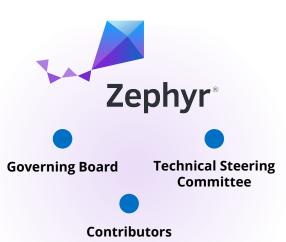


Vibrant Ecosystem





Development Tools





Applications & Middlewares



Training & Consulting



Firmwares & Libraries

© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.

Development Tools Compilers LAUTERBACH **Emulation / Simulation** RENODE WOKWI

Ecosystem // **Dev Tools**





Debuggers / Tracing Tools



Zephvr



SEGGER



000

Ecosystem // Training & Consulting





Training & Consulting



Firmwares & Libraries





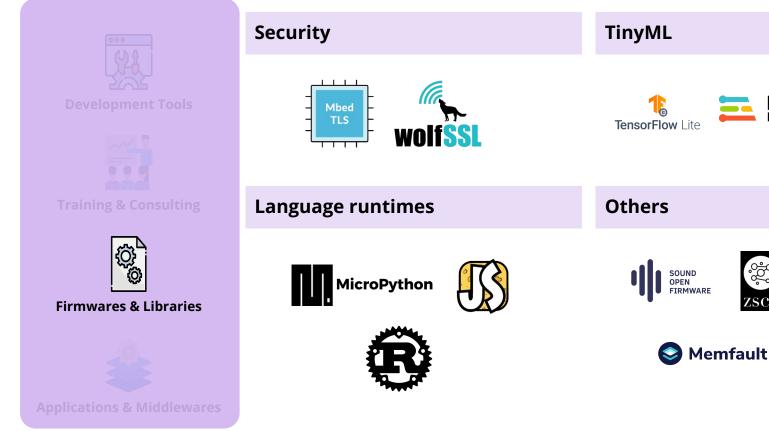


Zephvr

Ecosystem // Firmwares & Libraries

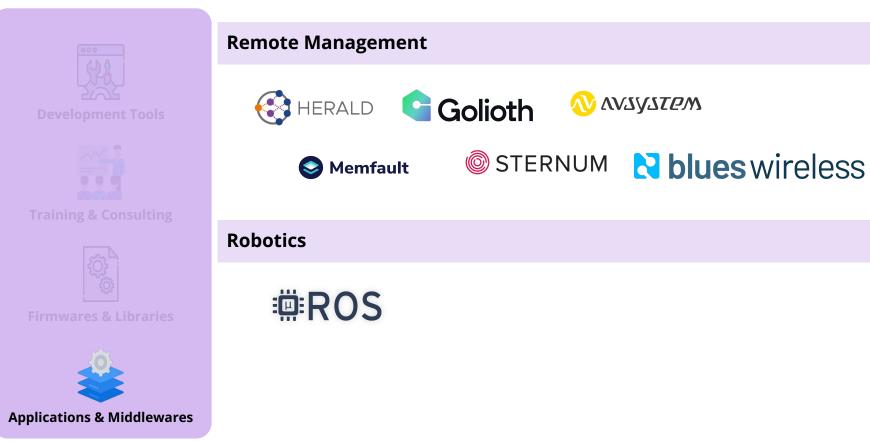


EDGE IMPULSE



Ecosystem // Apps & Middlewares





SBOMs at scale - see RENODE Dashboard: 3 SBOMs Included by default on each build.



| ZEPHYR DASHBOARD | This dashboard is generated by a Cl rur to run them in <mark>Renode.</mark> | which builds all boa | rds supporte | d in <mark>Zephyr R</mark> | TOS and tries | |
|--|--|----------------------|--------------|----------------------------|--------------------------|-------------|
| STATUS MATRIX | | | | | | |
| BINARIES V | | | | | | |
| ZEPHYR HELLO WORLD | Q Search | 229 PASSED | 227 PASSED | 212 PASSED | 214 PASSED | 192 PASSED |
| ZEPHYR PHILOSOPHERS ZEPHYR SHELL TENSORFLOW LITE MICRO | BOARD NAME | HELLO WORLD | PHILOSOPHERS | SHELL MODULE | TENSORFLOW LITE MICRO | MICROPYTHON |
| MICROPYTHON | ARM (368) ^ | | | | | |
| ARCHITECTURE V | ARM64 (12) 🔨 | | | | | |
| ARM | NIOS2 (1) ^ | | | | | |
| A R M 6 4 | | | | | | |
| NIOS2 | RISCV (21) 🗸 | | | | | |
| RISCV | | | | | | |
| SPARC | Andes ADP-XC7K AE350 | BUILT | BUILT | BUILT | BUILT | BUILT |
| X 8 6 | | | | | | |
| XTENSA | BeagleV Starlight JH7100 (NON-SMP) | PASSED | PASSED | PASSED | PASSED | BUILT |
| BUILD DETAILS | | | | | | |
| RE 27C686B7 | ESP32-C3 | BUILT | BUILT | BUILT | BUILT | BUILT |
| 98580F1C22 | Fomu - The FPGA-based Tomu | PASSED | PASSED | PASSED | PASSED | NOT BUILT |
| SUPPORTED IN RENODE? <u>Contact us</u> for renode Support services | GigaDevice GD32VF103C-STARTER | BUILT | BUILT | BUILT | NOT BUILT | NOT BUILT |

https://zephyr-dashboard.renode.io/



Interested to Learn More? Come Join Us!

Zephyr Community Overview:

<u>https://www.zephyrproject.org/community/</u>

Code on GitHub:

<u>https://github.com/zephyrproject-rtos/zephyr</u>

Mail Lists:

<u>https://lists.zephyrproject.org/g/main</u>

Discord (8000+ developers):

<u>https://chat.zephyrproject.org/ (https://discord.com/invite/Ck7jw53nU2)</u>



Zephyr Project

- **Open source** real time operating system
- Vibrant Community participation
- Vendor Neutral governance
- Permissively licensed Apache 2.0
- Cross-architecture with broad SoC and development board support.
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**
- Product development ready using LTS includes security updates
- Built with safety and security in mind

THELINUX FOUNDATION PROJECTS

Open Source, RTOS, Connected, Embedded Fits where Linux is too big





Questions?

www.zephyrproject.org



EMBEDDED IOT SUMMIT

THE LINUX FOUNDATION OPEN SOURCE SUMMIT

