Introduction to the Zephyr Project:
Unlocking Innovation with an Open Source RTOS

Thea Aldrich
thea@linux.com

Welcome!

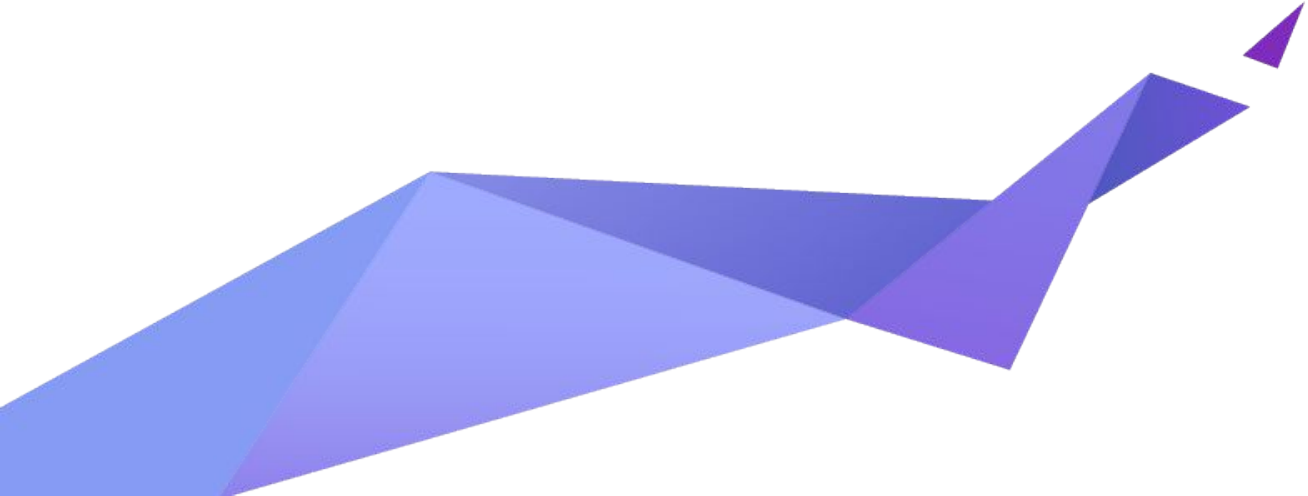
Zephyr™

Thea Aldrich

Zephyr Project Community Ambassador

@TheaClay

Welcome to the Zephyr Project



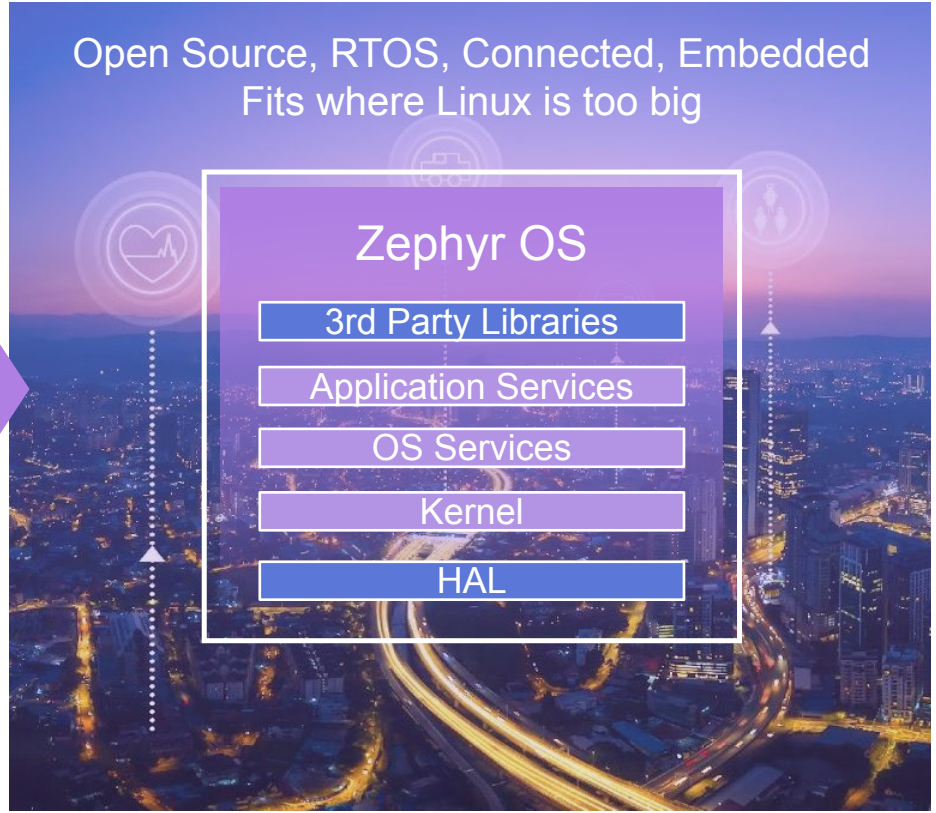
Vision Statement

Zephyr™

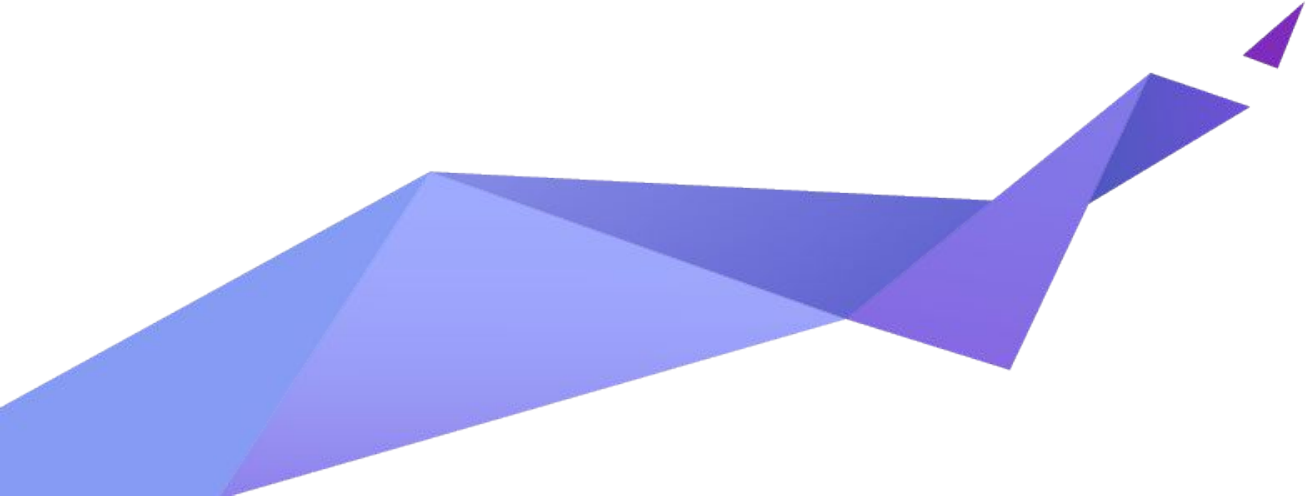
The Zephyr Project strives to deliver the **best-in-class RTOS** for connected resource-constrained devices, built to be secure and safe.

Zephyr Project

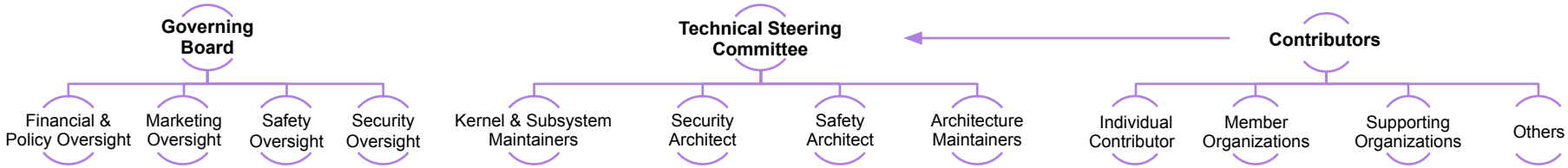
- **Open source** real time operating system
- **Permissively** licensed - Apache 2.0
- **Vendor Neutral** governance
- **Vibrant Community** participation
- **Cross-architecture** with broad SoC and development board support.
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**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



The Zephyr Project Community



Zephyr Project Governance



Goal: Separate business decisions from meritocracy, technical decisions

Governing Board

- Decides project goals and strategic objectives
- Makes business , marketing and legal decisions
- Prioritizes investments and oversees budget
- Oversees marketing such as PR/AR, branding, others
- Identifies member requirements

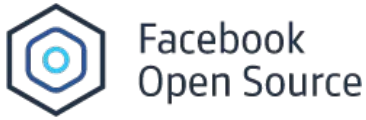
Technical Steering Committee

- Serves as the highest technical decision body consisting of project maintainers and voting members
- Sets technical direction for the project
- Coordinates X-community collaboration
    - Sets up new projects
    - Coordinates releases
    - Enforces development processes
    - Moderates working groups
- Oversees relationships with other relevant projects

Community

- Code base open to all contributors, need not be a member to contribute.
- Path to committer and maintainer status through peer assessed merit of contributions and code reviews
- Ecosystem enablement

Zephyr Project Members



and more...

Growing a Diverse Vendor-Neutral Community!

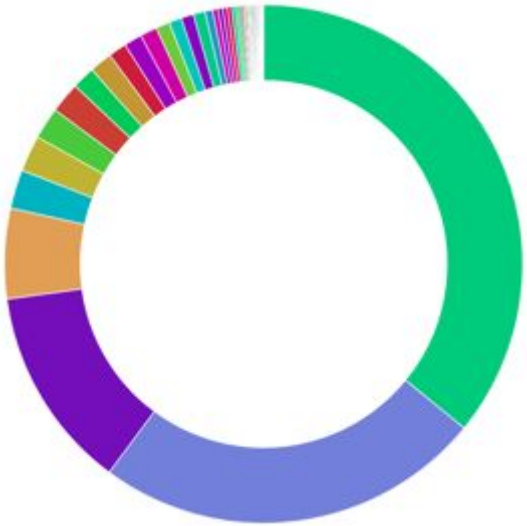
Lifetime project participation

Authors
- 2016/2: 80
- 2021/6: 979

Commits
- 2016/2: 2,806
- 2021/6: 52,999

Boards
- 2016/2: 4
- 2021/1: 250+

Company Participation over the last 12 months



- Intel
- Nordic Semicondu...
- Linaro
- (Unknown)
- Oticon
- NXP
- Independent
- Foundries
- ST Microelectronics
- Peter Bigot
- Baylibre
- Synopsys
- PHYTEC Messtech...
- Vestas
- Nokia
- LOBECO
- Nexiot
- Exusia
- Antmicro
- Centaur Analytics
- MLIPA
- Dialog Semicondu...
- SiFive
- ОАО ТриА
- Embarcados
- Grinn
- lemonbeat
- MRobot
- Codecoup
- Creative Dock
- Microchip Technol...
- NetEase
- Electronut Labs
- Laczen
- UNISOC
- Sheeld
- teenage engineering
- AMETEK
- Demant
- Korner

Vibrant, Active & Global Community

> 5600 Followers on Twitter

zephyrproject.org

Follow

Zephyr Project
@ZephyrIoT

An open source project to build a real-time operating system (RTOS) for the Internet of Things (IoT).

San Francisco, CA · zephyrproject.org · Joined February 2016

582 Following **5,640** Followers

> 2600 Active on LinkedIn

Zephyr™

The Zephyr Project
The Zephyr Project is an open source RTOS built for resource constrained devices.
Information Technology & Services · San Francisco, CA · 2,621 followers

> 2800 Active on Slack

#general
1 | Welcome to the Zephyr Project!

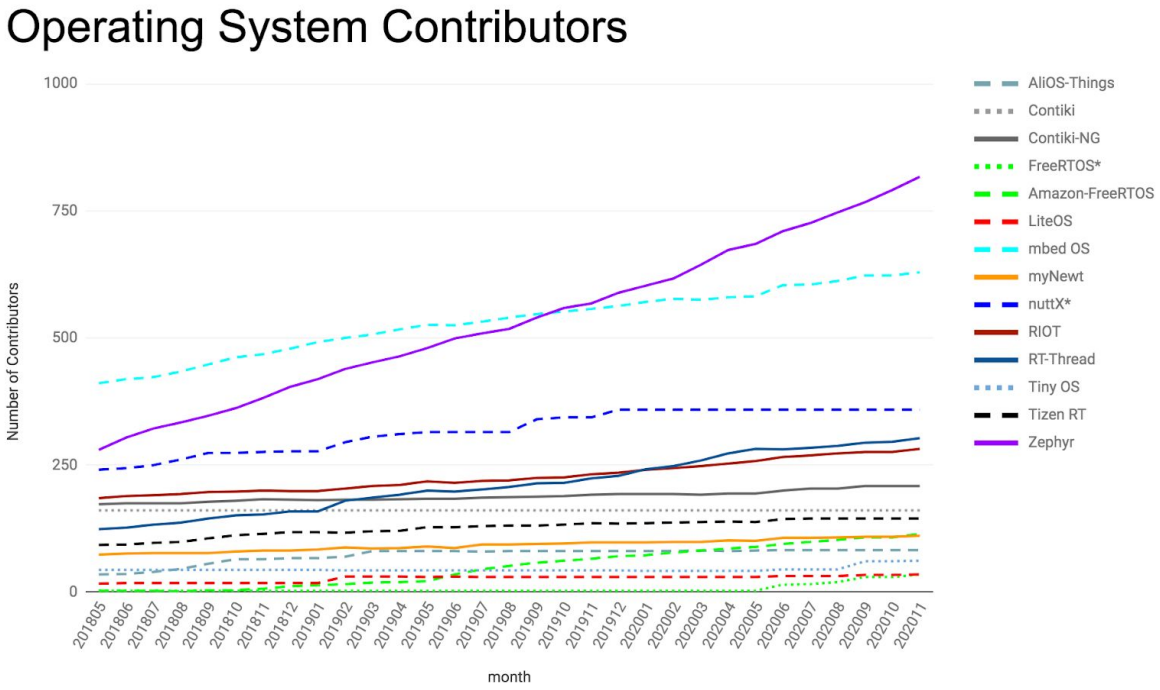
2,817

Saturday, May 22nd

Aveek Basu 9:26 AM
Can someone please suggest what would be the best board to start with for learning/playing around with Zephyr for a newbie...
L 11 replies Last reply 10 days ago

> 335 Members on WeChat Group

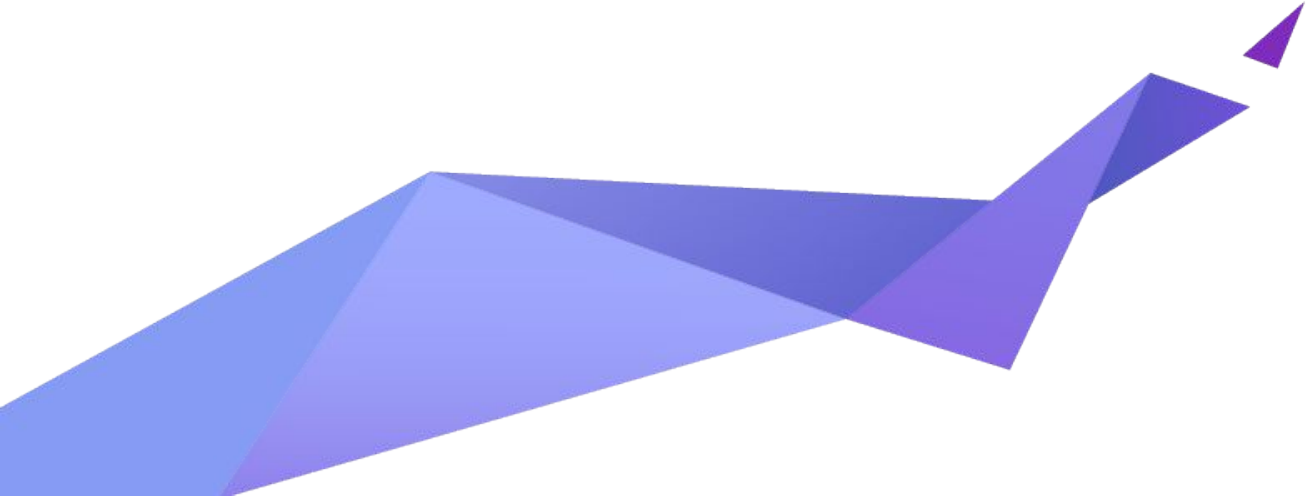
Growing Community Momentum



Github Web Traffic

2 weeks of traffic to github.com/zephyr code repository as of **2021/6/3**

Participating in the Zephyr Project



Zephyr General Information

Membership:

- https://www.zephyrproject.org/become-a-member/

Github:

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

Mail Lists:

- https://lists.zephyrproject.org/g/main

Slack:

- http://slack.zephyrproject.org/

Zephyr Project Community Guidelines

Orientation:

- https://www.zephyrproject.org/community/
- https://docs.zephyrproject.org/latest/index.html

Contribution Guidelines:

- https://docs.zephyrproject.org/latest/contribute/index.html

Code of Conduct:

- https://github.com/zephyrproject-rtos/zephyr/blob/master/CODE_OF_CONDUCT.md

Contribution Workflow:

- https://docs.zephyrproject.org/latest/contribute/index.html#contribution-workflow

Zephyr Project Documentation and Guides

Documentation:

- https://docs.zephyrproject.org/latest/index.html

Wiki:

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

Getting Started Guide

- https://docs.zephyrproject.org/latest/getting_started/index.html

Application Development:

- https://docs.zephyrproject.org/latest/application/index.html

Technical Call Information

Be part of the discussion

- Learn more about the features and functionality on the roadmap
- Help shape the direction of the code base
- Professional engagement and learning
- Fastest path to getting your PR accepted

Technical Call Schedule

Meeting Schedule	
Technical Steering Committee	Weekly, Wednesdays
Process Improvement Forum	Weekly, Wednesdays
Testing Working Group	Weekly, Mondays
Bug Triage/Release Readiness	Weekly, Tuesdays
API Committee	Weekly, Tuesdays
Zephyr Dev Meeting	Weekly, Thursdays
Marketing Committee	Bi-weekly, Mondays
Toolchain Committee	Bi-Weekly, Mondays
Networking Forum	Monthly, 1st Monday

Sample of Products Running Zephyr Today

Zephyr™

Grush Gaming Toothbrush

Proglove

Rigado IoT Gateway

Adero Tracking Devices

Distancer

OB-4

Ellcie-Healthy Smart Connected Eyewear

Intellinium Safety Shoes

GNARBOX 2.0 SSD

HereO Core Box

Safety Pod

Oticon More

hereO Smartwatch

Point Home Alarm

RUUVI Node

Anicare Reindeer Tracker

Sentrius

See.Sense AIR

Board Support – 250+ and growing

Zephyr™

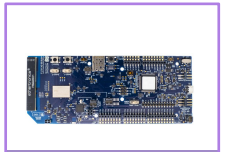

Arduino Due


Nucleo 103RB


Adafruit Feather

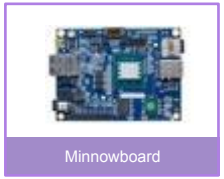

Nucleo64 L476RG


Nucleo F411RE


NRF91 pca10090


Nucleo F334R8


Synopsys EMSK


Minnowboard


Altera MAX10

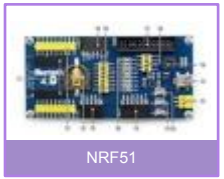

Nucleo 401RE


Vega Board


ARM V2M MPS2


STM3210c


Atmel SAM E70


NRF51


NXP FRDM K64F


NRF52


Seed Carbon


TI Launchpad Wifi


BBC Microbit


STM32373c

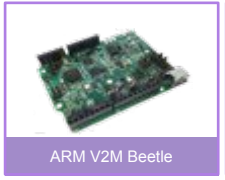

Redbear BLE Nano

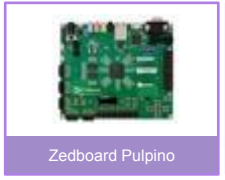

96b Neon Key


STM32 Olimexino


STM Mini A15


Seeed Nitrogen


ARM V2M Beetle


Zedboard Pulpino


NXP FRDM-KW41Z

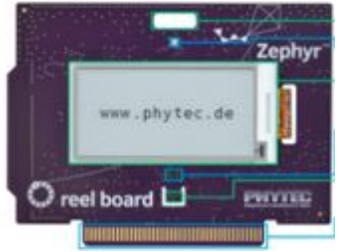

SiFive HiFive1


NXP i.MX RT1050

http://docs.zephyrproject.org/boards/boards.html

Development Boards Shipping with Zephyr Today

GEPS - Nordic Thingy91

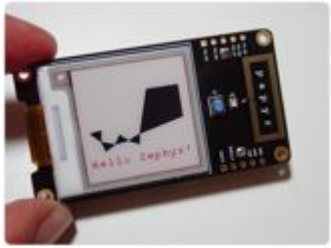


Phytec Reel Board

Icarus (Adafruit Feather) - Actinius

Antmicro Badge

Phytec Link Board BASE



Electronuts Papyr

SonicBoard BLE

Zephyr Supported Hardware Architectures

Zephyr™

ARC Synopsys

arm
Cortex-M, Cortex-R
& Cortex-A

intel®
X86 & x86_64

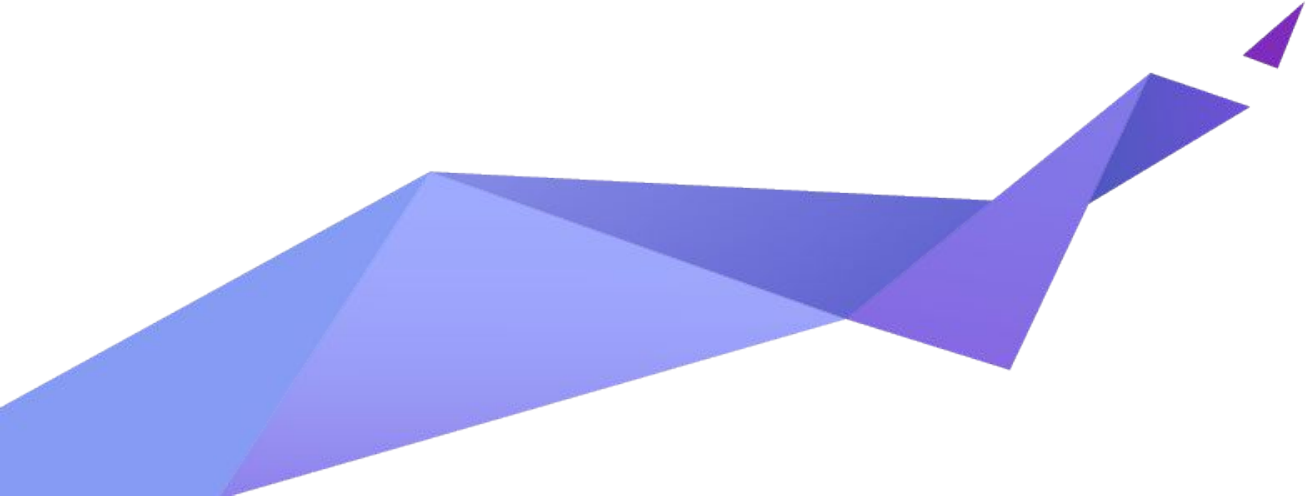
Nios® II
Processor

RISC-V
32 & 64 bit

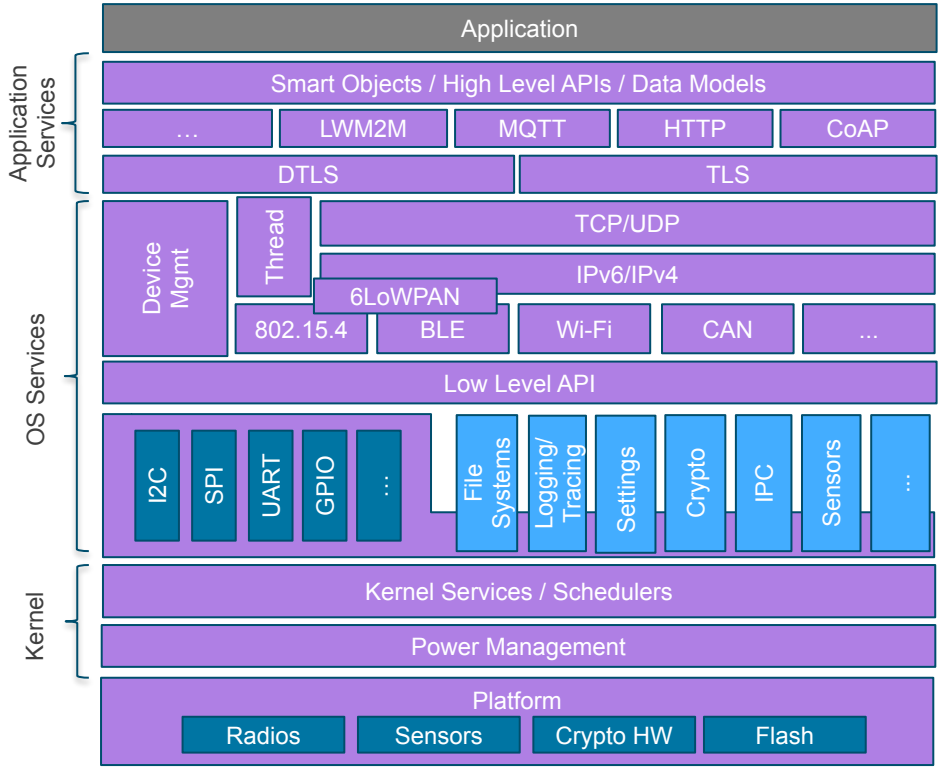
SPARC

tensilica
Xtensa

Zephyr OS Basics



Architecture

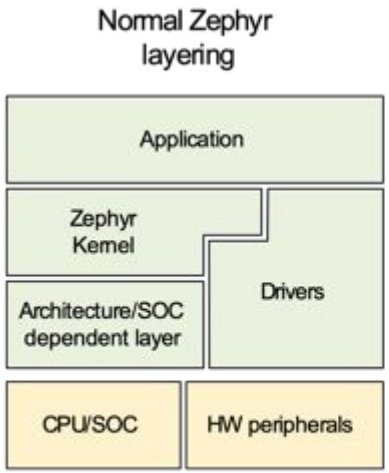


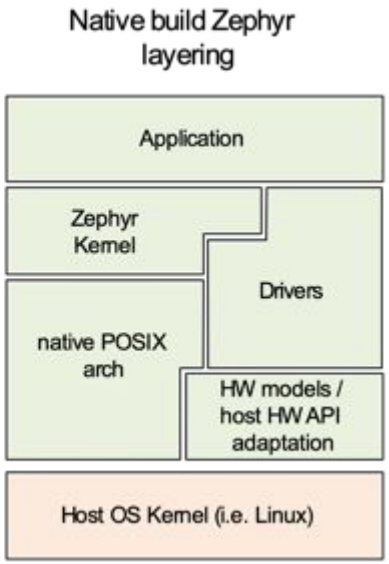
- Highly Configurable, Highly Modular
- Cooperative and Preemptive Threading
- Memory and Resources are typically statically allocated
- Integrated device driver interface
- Memory Protection: Stack overflow protection, Kernel object and device driver permission tracking, Thread isolation
- Bluetooth® Low Energy (BLE 5.1) with both controller and host, BLE Mesh
- 802.15.4 OpenThread
- Native, fully featured and optimized networking stack

Fully featured OS allows developers to focus on the application

Native Execution on a POSIX-compliant OS

- **Build Zephyr as native Linux application**
- Enable large scale simulation of network or Bluetooth tests without involving HW
- Improve test coverage of application layers
- Use any native tools available for debugging and profiling
- Develop GUI applications entirely on the desktop
- Optionally connect to real devices with TCP/IP, Bluetooth, and CAN
- **Reduce requirements for HW test platforms during development**



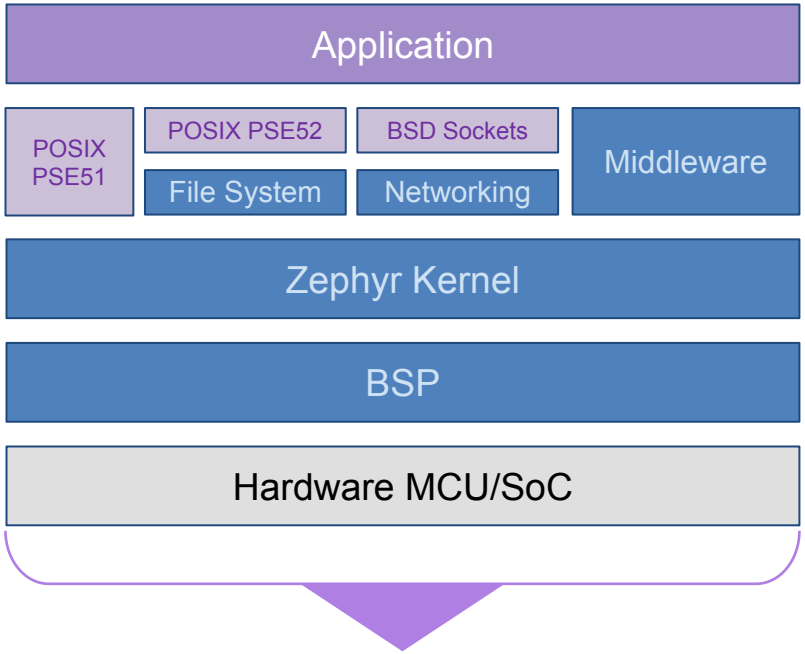


POSIX API on Zephyr

Provides familiar API to non-embedded programmers, especially to Linux developers

Enable re-use (portability) of existing libraries based on POSIX APIs

- Provides efficient subset appropriate for small (MCU) embedded systems
- POSIX API subset is increasingly popular operating system abstraction layer (OSAL) for IoT
- Supports subsets of PSE51, PSE52, and BSD sockets API

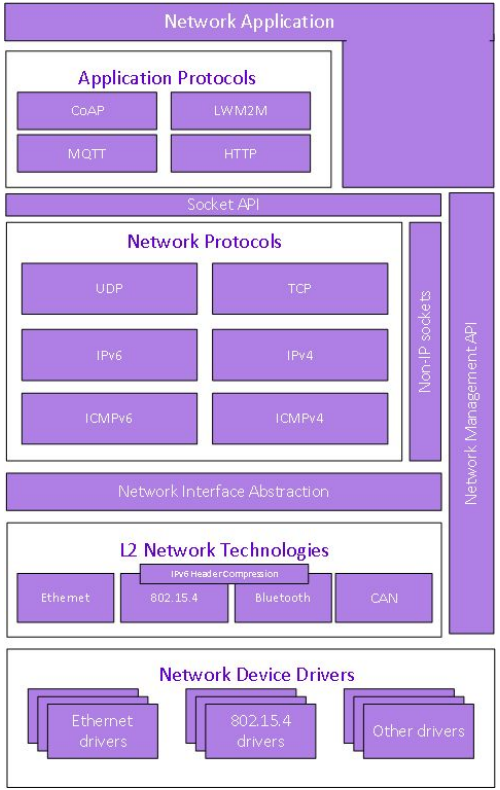


POSIX support in Zephyr

https://docs.zephyrproject.org/latest/guides/portability/posix.html

Native IP Stack

- Build from scratch for Zephyr
  - Using Zephyr native kernel concepts
- Dual mode IPv4/v6 stack
  - DHCP v4; IPv4 autoconf; IPv6 SLAAC; DNS; SNTP
- Multiple network interfaces support
- Time Sensitive Networking support
  - 802.1QAV API
  - 802.1AS (gPTP, generalized Precision Time Protocol)
- BSD Sockets-based API
  - TLS/DTLS supported via setsockopt call
  - RAW socket support for IP and non-IP traffic
- Supports IP offloading
  - Transparent for application using Socket API
- Compliance and security tested
  - >500 automated tests for TCP level using commercial products like IWL Maxwell Pro



Zephyr Networking Features

High-Level Protocols

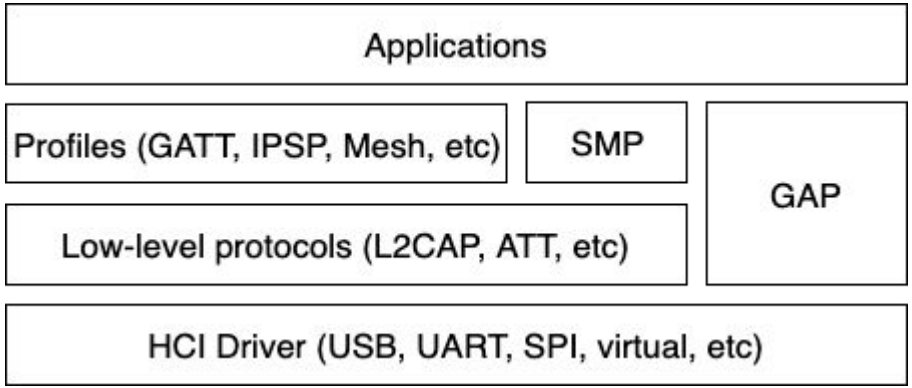
- CoAP v1
- MQTT Client v3.1.1
- HTTP
  - As of Zephyr 2.0 server is implemented using CivetWEB library
  - Native HTTP client
  - Websocket client
- SOCKS5
- LWM2M
- Thread
  - Supported by OpenThread project

Supported technologies

- Ethernet
- Ethernet over USB
- WiFi with IP offload
- IEEE 802.15.4 with 6Lo
- Bluetooth LE with 6Lo
- CANbus with 6Lo
- PPP

Bluetooth Host and Mesh

- Bluetooth 5.1 compliant
- Low Energy & experimental Bluetooth Classic
- Multiple HCI transports
- Qualified (as of 1.14.1) for LE and Mesh
- Can be built separately or combined with the controller
- Active community developing upcoming standards
- Mesh & GATT reference stack in Bluetooth SIG training materials



Bluetooth Low Energy Controller

Zephyr™

Second-generation open source BLE software Controller:

- Bluetooth 5.1 compliant and qualified (v1.14.1)
- Split design with Upper and Lower Link Layers
- Support for multiple BLE radio hardware architectures
  - Nordic nRF5 on Arm Cortex-M
  - VEGAboard on RISC-V
  - Proprietary radios (downstream only)
- Support for both Big and Little-Endian architectures
- Asynchronous handling of procedures in the ULL
- Enhanced radio utilization (99% on continuous 100ms scan)
- Latency resilience: Approx 100uS vs 10uS, 10x improvement over 1st gen
- CPU and power usage: About 20% improvement over 1st gen
- Multiple advertiser and scanner instances

Zephyr USB Device Stack

- Supports multiple MCU families (STM32, Kinetis, nRF, SAM, …)
- USB 2.0 support
- Full and High speed support
- Supported classes:
  - CDC ACM, ECM, EEM
  - RNDIS
  - HID
  - Mass Storage
  - Bluetooth
  - Device Firmware Update
- Tight integration with the RTOS
- Flexible descriptor instancing
- Native execution support for emulated development on Linux
- WebUSB support

Getting Started with west

Zephyr's "meta-tool" or "swiss army knife," used for many common development workflows.

An extensible command line tool for managing a Zephyr workspace:
https://docs.zephyrproject.org/2.3.0/guides/west/index.html

Recommended but not required:
https://docs.zephyrproject.org/2.3.0/guides/west/without-west.html

Developed in its own git repository:
https://github.com/zephyrproject-rtos/west

West Documentation and Guides

West page in the Zephyr guides and Troubleshooting west

Or

`$ west help`

List all commands and one line help for each (including extensions).

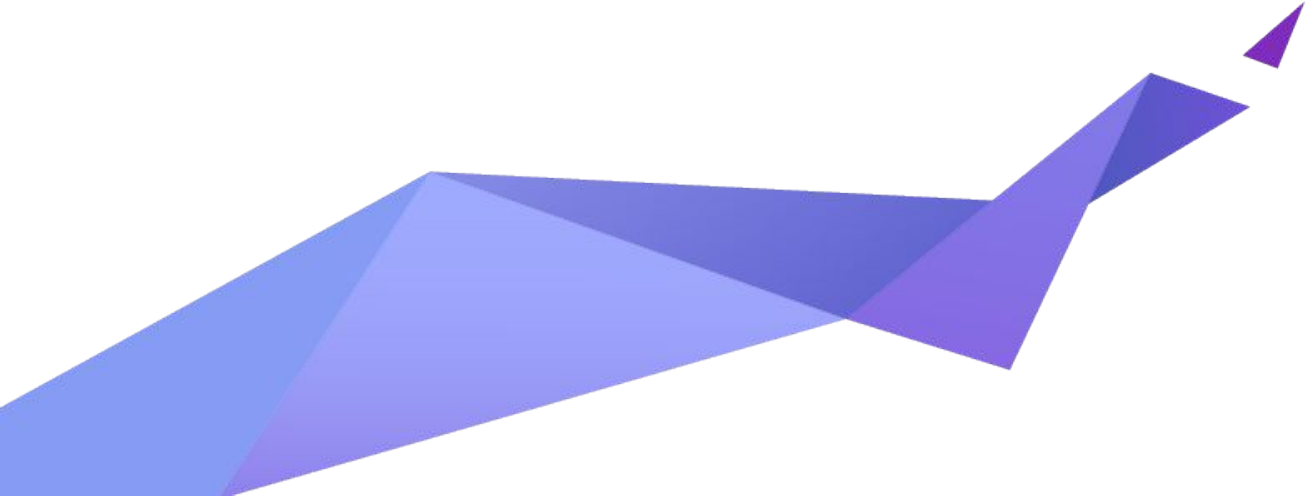
`$ west <command> help`

Help for a specific <command>, like `west help init`

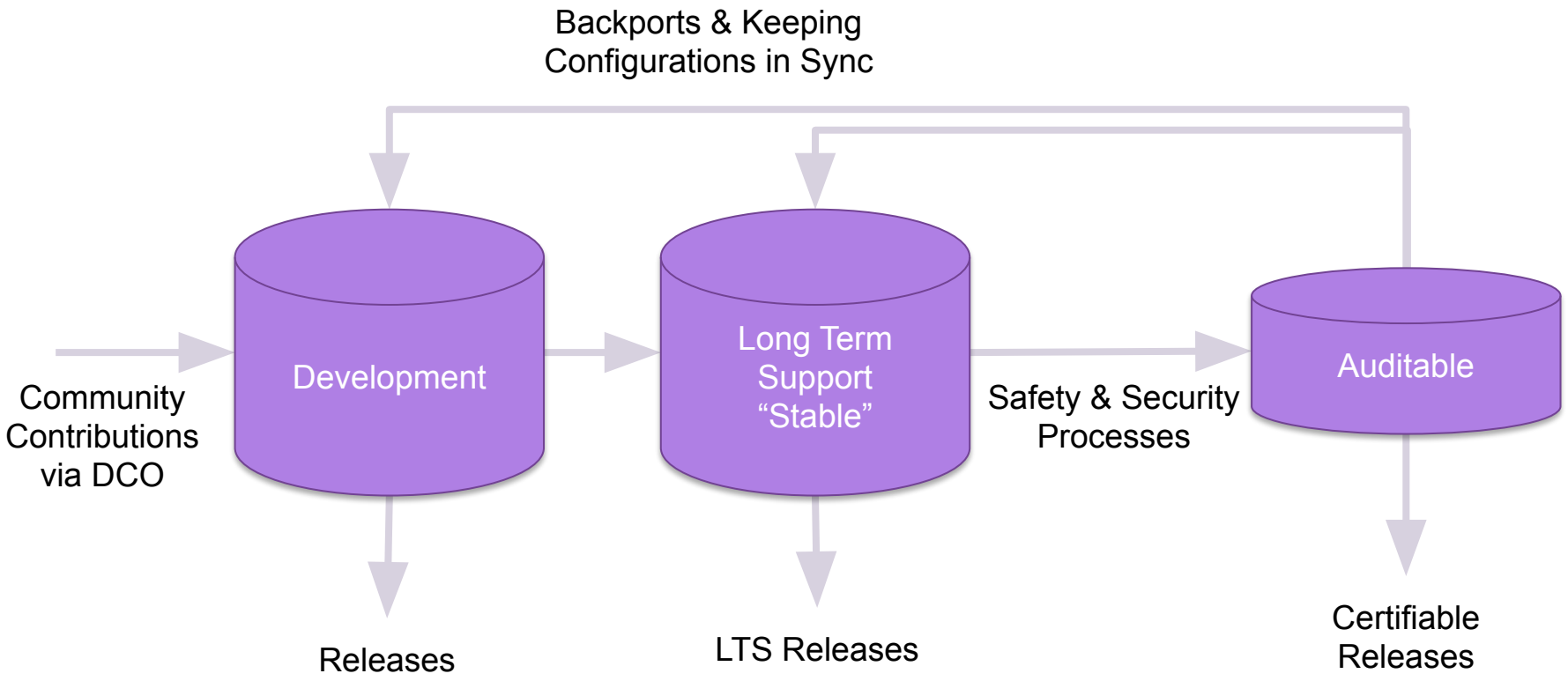
`$ west -v <command>`

Enable verbose output for `<command>`, like `west -v init`

Zephyr OS Releases



Code Repositories



Zephyr OS: Long Term Support (LTS - 1.14)

zephyrproject-rtos / zephyr

Unwatch 319 Star

Code | Issues 906 | Pull requests 431 | Actions | Projects 9 | Wiki | Security | Insights

Releases | Tags

zephyr-v1.14.0
cebe115
Unverified

Zephyr 1.14.0

galak released this on Apr 16 · 5126 commits to master since this release

We are pleased to announce the release of Zephyr kernel version 1.14.0.

Major enhancements with this release include:

- The Zephyr project now supports over 160 different board configurations spanning 8 architectures. All architectures are rigorously tested and validated using one of the many simulation platforms supported by the project: QEMU, Renode, ARC Simulator, and the native POSIX configuration.
- The timing subsystem has been reworked and reimplemented, greatly simplifying the resulting drivers, removing thousands of lines of code, and reducing a typical kernel build size by hundreds of bytes. TICKLESS_KERNEL mode is now the default on all architectures.
- The Symmetric Multi-Processing (SMP) subsystem continues to evolve with the addition of a new CPU affinity API that can "pin" threads to specific cores or sets of cores. The core kernel no longer uses the global irq_lock on SMP systems, and exclusively uses the spinlock API (which on uniprocessor systems reduces to the same code).
- Zephyr now has support for the x86_64 architecture. It is currently implemented only for QEMU targets, supports arbitrary numbers of CPUs, and runs in SMP mode by default, our first platform to do so.
- We've overhauled the Network packet net-pkt API and moved the majority of components and protocols to use the BSD socket API, including MQTT, CoAP, LWM2M, and SNTP.

zephyrproject-rtos / zephyr

Unwatch 319 Star

Code | Issues 906 | Pull requests 430 | Actions | Projects 9 | Wiki | Security | Insights

Releases | Tags

Latest release
zephyr-v1.14.1
9591025

Zephyr 1.14.1

nashif released this 26 days ago · 5126 commits 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.

Security Vulnerability Related

The following security vulnerability (CVE) was addressed in this release:

- Fixes CVE-2019-9506: The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.

Bluetooth

- Qualification:
  - 1.14.x Host subsystem qualified with QDID 139258
  - 1.14.x Mesh subsystem qualified with QDID 139259
  - 1.14.x Controller component qualified on Nordic nRF52 with QDID 135679

Issues Fixed

These GitHub issues were addressed since the previous 1.14.0 tagged

zephyrproject-rtos / zephyr

Unwatch 340 Star

Code | Issues 1,018 | Pull requests 428 | Actions | Projects 10 | Wiki | Security 0 | Ins

Releases | Tags

Latest release
v1.14.2
035ab2b

Compare

Zephyr LTS 1.14.2 (Maintenance Release)

nashif released this 25 days ago · 11296 commits to master since this release

This is an LTS maintenance release with fixes.

Security Vulnerability Related

The following security vulnerabilities (CVEs) were addressed in this release:

- CVE-2020-10019
- CVE-2020-10021
- CVE-2020-10022
- CVE-2020-10023
- CVE-2020-10024
- CVE-2020-10027
- CVE-2020-10028

More detailed information can be found in:
https://docs.zephyrproject.org/latest/security/vulnerabilities.html

Issues Fixed

These GitHub issues were addressed since the previous 1.14.0 tagged release:

Delivering bug fixes and latest security updates!

Zephyr OS: Long Term Support (LTS - 1.14)

Zephyr™

It is:

- **Product Focused**
- **Current with latest Security Updates**
- **Compatible with New Hardware**: We will make point releases throughout the development cycle to provide functional support for new hardware.
- **Tested**: Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- **Supported** for 2 years

It is *not*:

- **A Feature-Based Release**: focus on hardening functionality of existing features, versus introducing new ones.
- **Cutting Edge**

Zephyr OS: Auditable

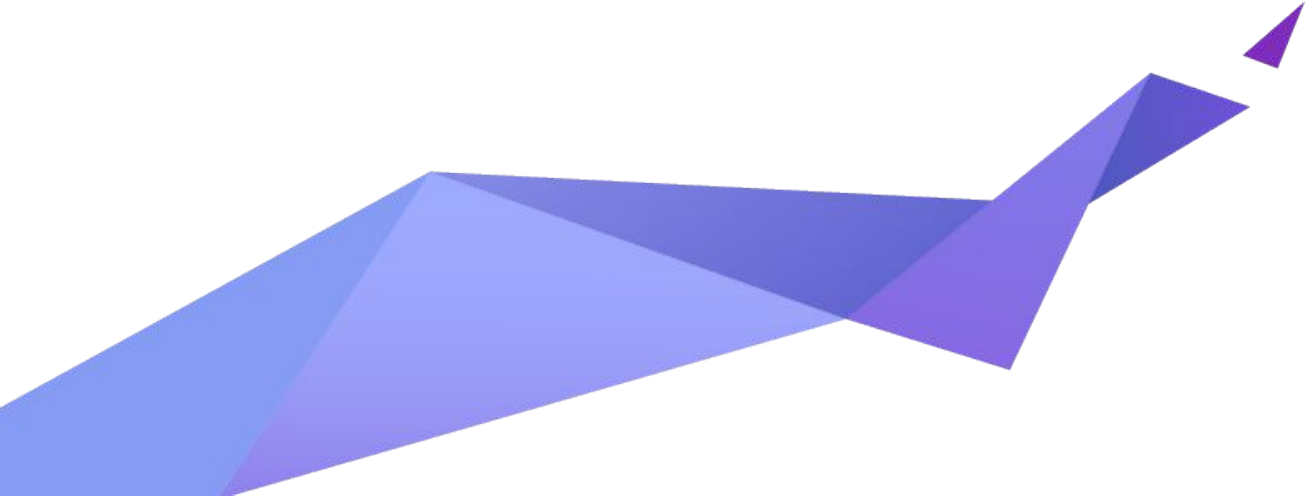
An auditable code base will be established from a subset of the **Zephyr OS LTS**.

- 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

Zephyr’s Security Focus

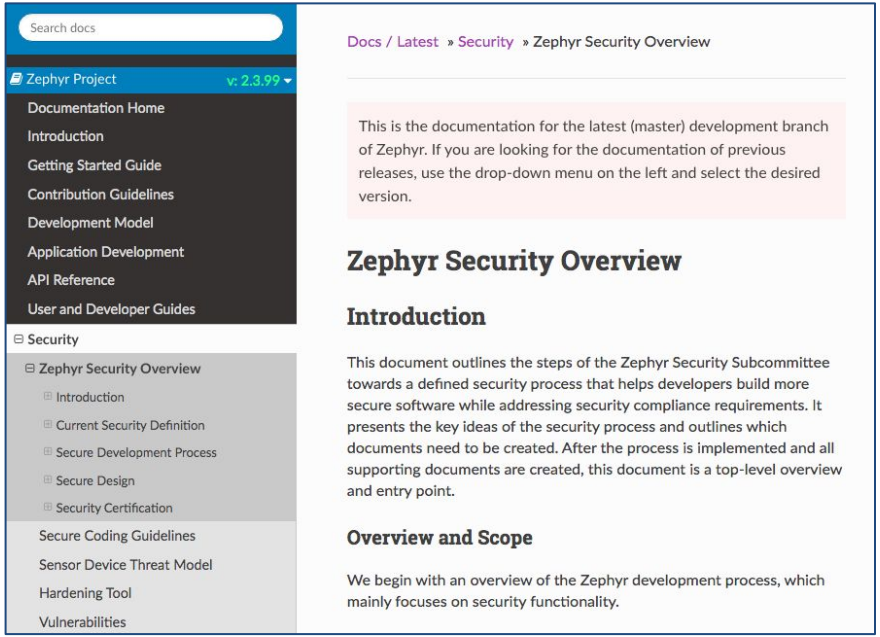


Building in Security for LTS & Auditable

- Established Security Committee in 2016 – meets bi-weekly.
- Secure Coding Practices have been documented for project.
- Zephyr Project registered as a CVE Numbering Authority with MITRE.
- Security Working Group has vulnerability response criteria publicly documented
  - addressed weaknesses and vulnerabilities already
- “Gold” Best Practices for projects as defined by CII
  - https://bestpractices.coreinfrastructure.org/projects/74
- Leveraging Automation to prevent regressions:
  - Weekly Coverity Scans to detect bad practices in imported code
  - MISRA scans being incorporated, to evolve to conformance and address issues.

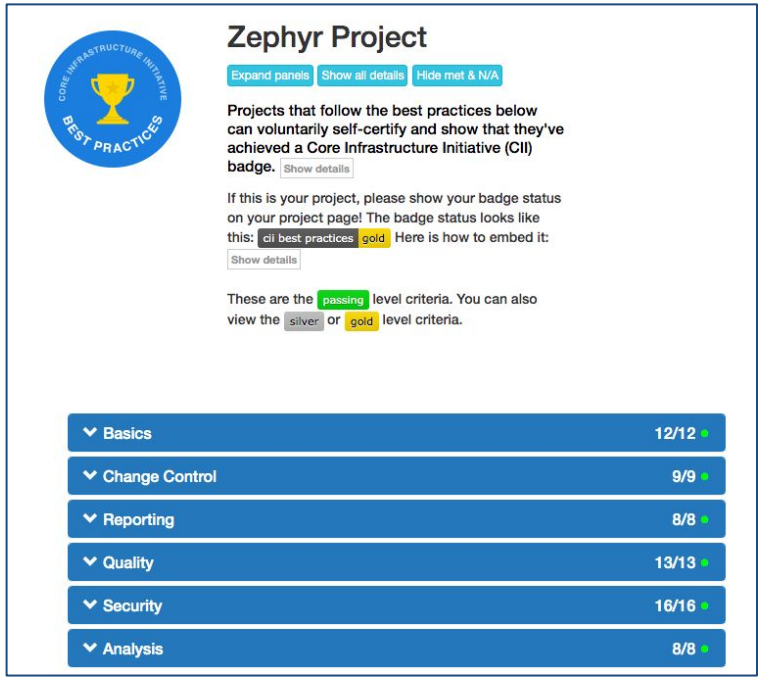
Project Security Documentation

- [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



CII Gold Badge

- Core Infrastructure Initiative Best Practices Program
- Awards badges based on “project commitment to security”
- Mostly about project infrastructure: is project hosting, etc following security practices
- Zephyr achieved gold Feb, 2019



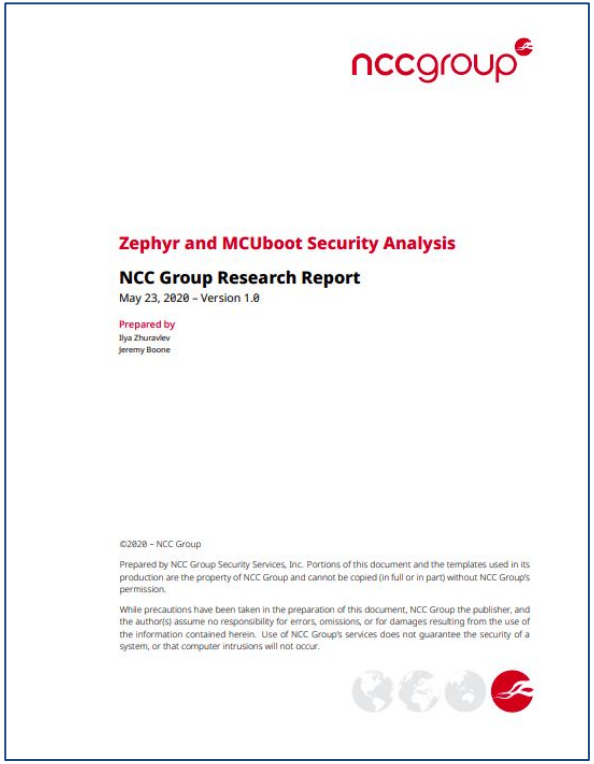
CVE Numbering Authority with PSIRT

- PSIRT is Subset of Security Subcommittee
- CNA: CVE Numbering Authority
- Registered with MITRE as the numbering authority for the project. We issue our own CVEs
- Must satisfy MITRE documentation and process requirements

Zephyr Project	Zephyr project components, and vulnerabilities that are not in another CNA's scope	vulnerabilities@zephyrproject.org Zephyr Disclosure Policy Zephyr Security Advisories	Vendors and Projects

Recent Security Report

- NCC Group reported ~26 issues
- Critical, High and Medium made into JIRA tickets
- These have now been fixed
- Embargo is past, everything updated now in the vulnerability report page
- Most resulted in 1 or more CVEs being reported



nccgroup

Zephyr and MCUboot Security Analysis

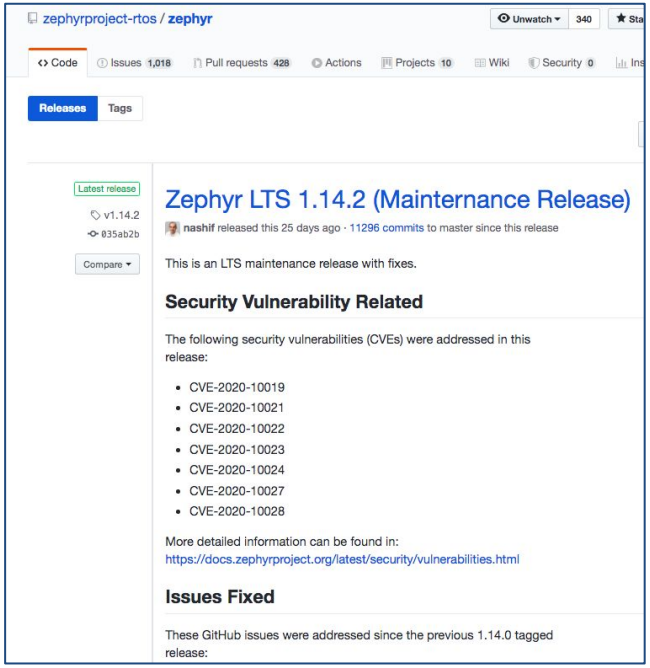
NCC Group Research Report

May 23, 2020 – Version 1.0

Prepared by
Ilya Zhuraviev
Jeremy Boone

Results from the Report

- Most issues were fixed in reasonable time and included in releases
- One issue, recommendation is to disable
- Increased embargo from 60 to 90 days
  - Zephyr isn't an end product, vendors need time to incorporate fixes into products
  - Zephyr needs alert system to notify vendors
- Continue to improve process



Zephyr Crypto Drivers

- Same API for different implementations
  - Provided by hardware
    - Atmel ATAES132A
    - ST STM32_crypt
    - Nordic nRF_AEB
  - Provided by software modules
    - mbed TLS feature-rich
    - TinyCrypt very small footprint

Zephyr PSIRT: Ready to Respond

Advisory Issued by project on 20201208:

Zephyr current release (2.4) does **not use** Fnet or other stacks.

The Zephyr LTS release 1.14 contains an implementation of the TCP stack from Fnet.

- Of the vulnerabilities reported in Fnet, 2, CVE-2020-17468, 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.

https://www.zephyrproject.org/zephyr-security-update-on-amnesia33/

WIP: Improve vulnerability tracking automation

An official website of the United States government Here's how you know

ICS Advisory (ICSA-21-119-04)

More ICS-CERT Advisories

Multiple RTOS (Update A)

Original release date: May 06, 2021 | Last revised: May 10, 2021

Print Tweet Send Share

--------- Begin Update A Part 3 of 3 ---------

- Micrium uC/LIB – Update available.
- Zephyr Project: Update to 2.5 or later . Patches available for prior supported versions. See the Zephyr security advisory for more information.

--------- End Update A Part 3 of 3 ---------

Security Advisories

View information about security vulnerabilities from this repository's maintainers.

✓ 11 Published

Integer Overflow in memory allocating functions GHSA-94vp-8gc2-rm45 published 19 days ago by d3zd3z	moderate severity
Remote Denial of Service in LwM2M do_write_op_tlv GHSA-g9mg-fj58-6fqh published 19 days ago by d3zd3z	moderate severity
Possible read out of bounds in dns read GHSA-mm57-9hqw-qh44 published 19 days ago by d3zd3z	critical severity
Malformed SPI in response for eswifi can corrupt kernel memory GHSA-hx4p-j86p-2mhr published 19 days ago by d3zd3z	high severity
Security problem with settings and littlefs GHSA-5qhg-j6wc-4f6q published 19 days ago by d3zd3z	low severity
Incorrect Error Handling in Bluetooth HCI core GHSA-gc66-xfrc-24qr published 19 days ago by d3zd3z	low severity
Missing Size Checks in Bluetooth HCI over SPI GHSA-hg2w-62p6-g67c published 19 days ago by d3zd3z	low severity
Improper Input Frame Validation in ieee802154 Processing GHSA-3gvq-h42f-v3c7 published 19 days ago by d3zd3z	high severity
FS: Buffer Overflow when enabling Long File Names in FAT_FS and calling fs_stat GHSA-7fhv-rgxr-x56h published 19 days ago by d3zd3z	moderate severity
Improper Handling of Insufficient Permissions or Privileges in zephyr GHSA-vf79-hqwm-w4xc published 19 days ago by d3zd3z	moderate severity

https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04

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

Cybersecurity Executive Order - 2021/5/12

WH.GOV

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

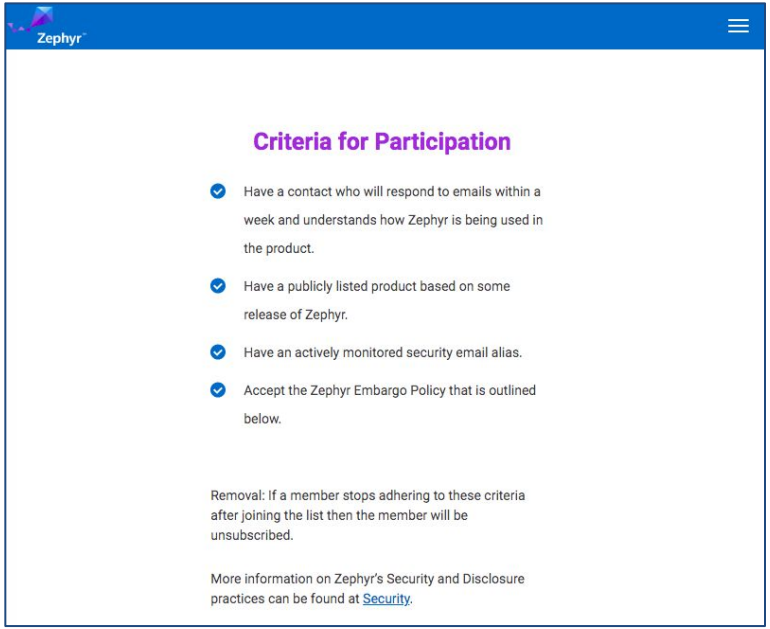
Zephyr Project provides a **SBOM on the source code** with each release, starting with version 2.5.

Starting with upcoming version 2.6, thanks to Steve Winslow, **product makers** using Zephyr are able to **automatically generate a SBOM for binaries they create** using SPDX document format (NTIA recognized SBOM format) which is accurate to the source file level (with included libraries & binaries). Details at: https://github.com/zephyrproject-rtos/zephyr/pull/34555

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ Section 4 (c)

Vulnerability Alert Registry

- For an **embargo to effective**, product makers need to be **notified early** so they can remediate
- Created [Vulnerability Alert Registry] for **product makers** can **register** to receive these alerts for **free.**
- **Goal:** Zephyr to fix issues within 30 days to **give vendors 60 days before publication of vulnerability**



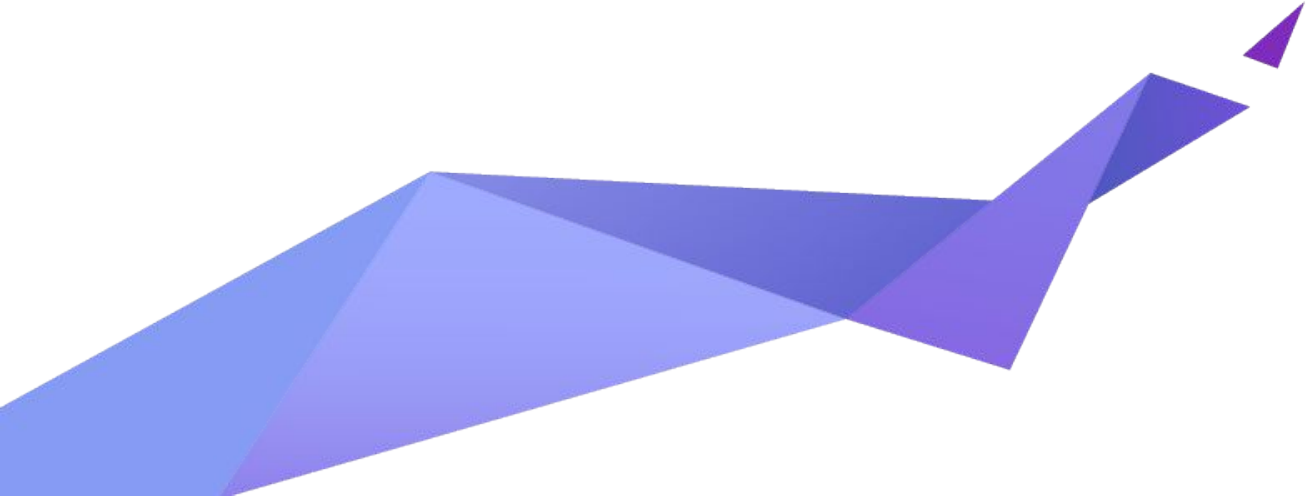
Zephyr Security Summary

- Established Security Committee at project launch in 2016 – meets bi-weekly.
- Secure Coding Practices have been publicly documented for project.
- Zephyr Project registered as a CVE Numbering Authority with MITRE since 2017.
- "Gold" Best Practices Badge criteria Core Infrastructure Initiative met in 2018
- Leveraging Automation to prevent security regressions:
  - Weekly Coverity Scans to detect bad practices in imported code
  - MISRA scans being incorporated, to evolve to conformance and address issues.
- Vulnerability Management in 2020
  - Vulnerability response criteria publicly documented
  - Product makers can register for free for notification of Zephyr

and now …. supporting **SBOM generation** in 2021

- Source SBOM's for releases and updates going forward from version 2.5
- Ability to automatically generate SBOM for built images included in version 2.6

Zephyr OS Safety Certification

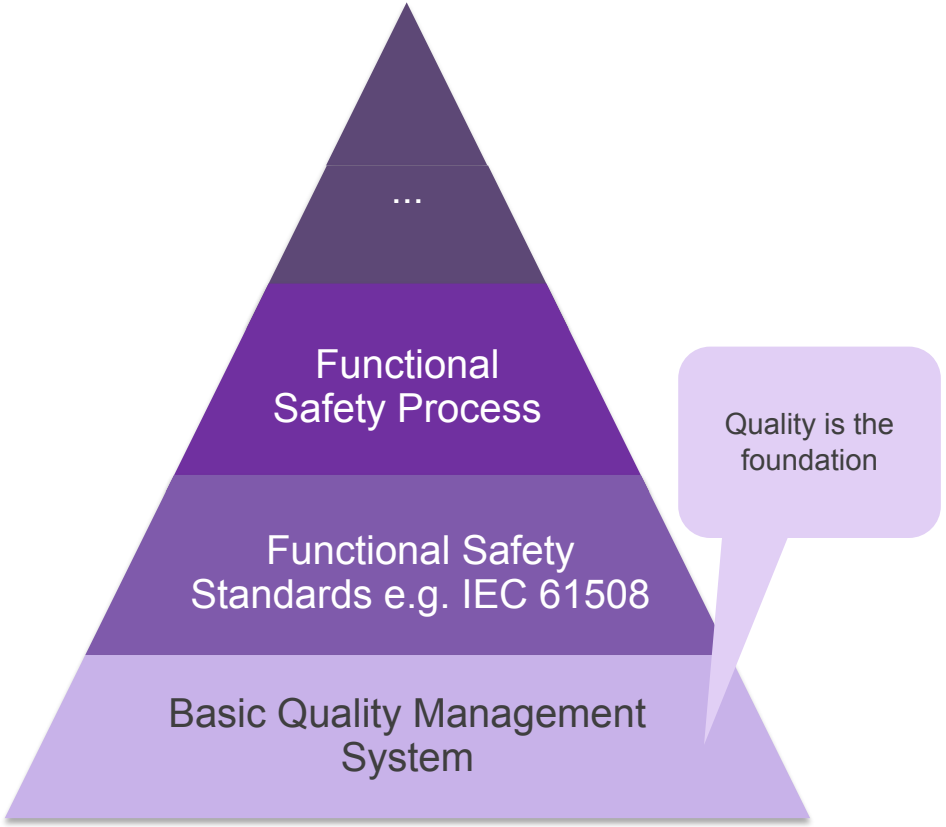


Building in Safety for LTS → Auditable

- Established **Safety Committee in 2019**, meets bi-weekly. Community that understands Safety considerations, and implications.
- Initial target was decided by Governing Board to be **IEC 61508** (it is a common basis for others standards that the members care about)
- Build on Coding Practices have been documented for the project to establish more general **Coding Guidelines**
- Passing Best Practices for **project quality** as defined by CII
  - https://bestpractices.coreinfrastructure.org/projects/74
- Leveraging Automation to **prevent regressions**:
  - Weekly Coverity Scans to detect bad practices in imported code
  - MISRA scans being incorporated, to evolve to conformance and address issues.
  - Looking for open source as well as commercial tooling to help here.

Zephyr OS: Development

- **Quality** is a **mandatory expectation** for software across the industry.
- Assumptions:
  - Software Quality is enforced across Zephyr project members
  - Compliance to internal quality processes is expected.
- **Software Quality** is not an additional requirement caused by functional safety standards.
- Functional safety considers Quality as an **existing pre-condition**.



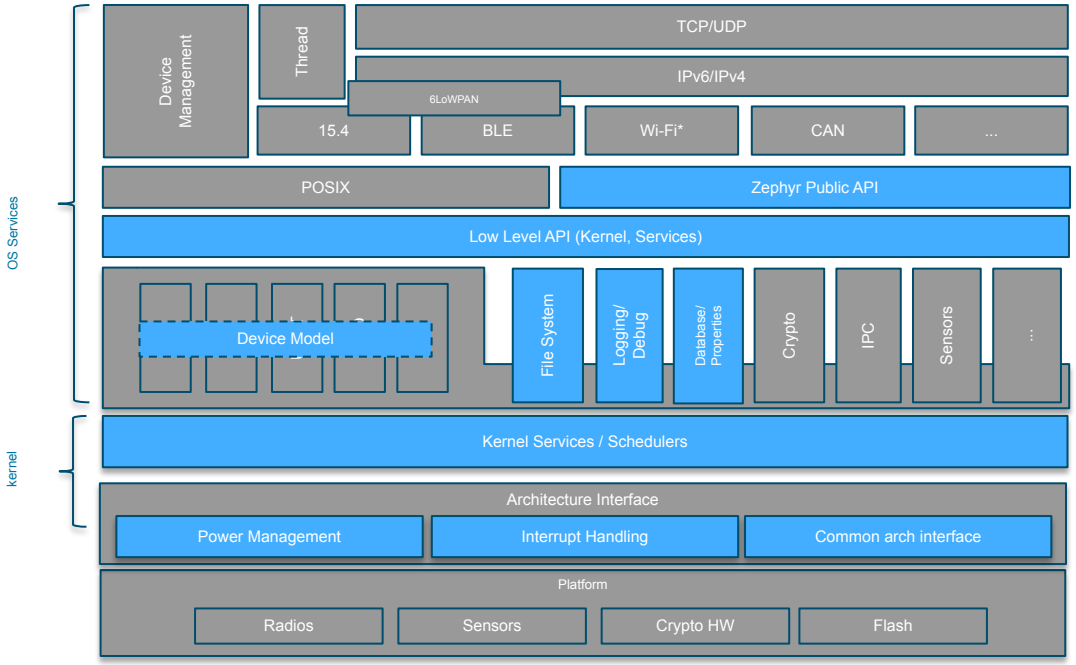
Zephyr OS: Initial Certification Focus

In scope

Out of scope

Scope will be **extended** to include **additional components** as determined by the safety committee

Some of the modules under consideration for the next iteration include: Crypto, IPC, Flash, etc.

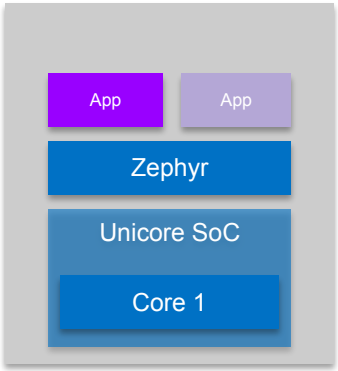


61508 Safety Collateral

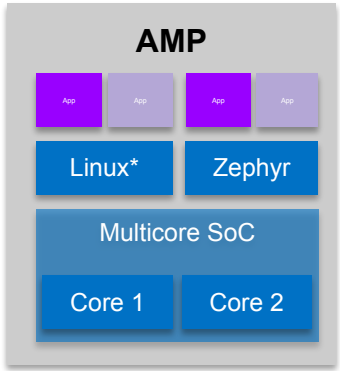
Zephyr™

Draft (pending approval by Certification Authority)				
Phase	**Assumed Collateral**	**Type of Doc**	**Owner**	**Sharing Model**
Safety Concept	Safety Plan and Safety Assessment Plan	Plan/Process	FSM	Platinum
	Verification / Validation / Integration Test Plans	Plan/Process	Testing WG	Public
	Software Development Plan	Plan/Process	TSC	Public
	Configuration and Change Management Plans	Plan/Process	TSC	Public
	Software Architecture and Module Design Specification	Plan/Process	TSC	Public
	Coding Guideline	Plan/Process	TSC	Public
	Tools Documentation	Plan/Process	TSC	Public
	Software Requirements	Code	TSC	Public
	Software Safety Requirements Specification	Result Artifact	Safety WG	Platinum
Detailed Test Phase	Tests (Integration, Arch / Module, Validation)	Code	TSC	Public
	Code Review Report	Result Artifact	Safety WG	Platinum
	Verification / Validation / Integration Test Reports	Result Artifact	Testing WG	Platinum
	Fault Injection Test Report	Result Artifact	Testing WG	Platinum
	Tools Classification	Result Artifact	Safety WG	Platinum
	Tools Validation	Result Artifact	Safety WG	Platinum
	Traceability Report	Result Artifact	Testing WG/FSM	Platinum
	Test Coverage Report	Result Artifact	Testing WG/FSM	Platinum
	Coding Guideline Compliance Report	Result Artifact	Safety WG	Platinum
	Safety Analysis (e.g., FMEA)	Result Artifact	FSM	Platinum
	Source Code	Code	TSC	Public
	Software User Manual	Result Artifact	TSC	Platinum
	Safety Manual	Result Artifact	FSM	Platinum
Silver members have limited access, restricted use to Platinum artifacts based on participation				

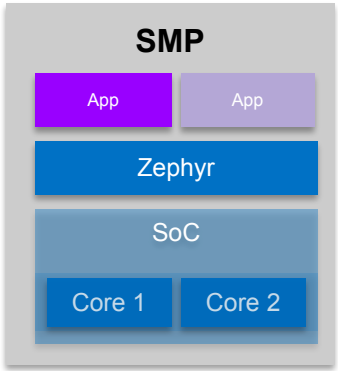
System Configurations



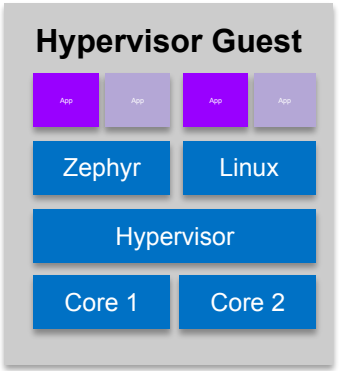
Single Core MCU



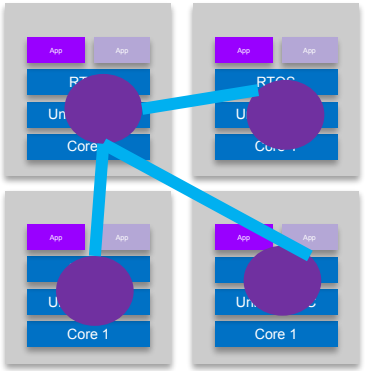
Supported with OpenAMP



Supported on some architectures



Supported with ACRN



Supported with Bluetooth & 15.4

Safety and security can apply to all these configurations

Zephyr™

www.zephyrproject.org