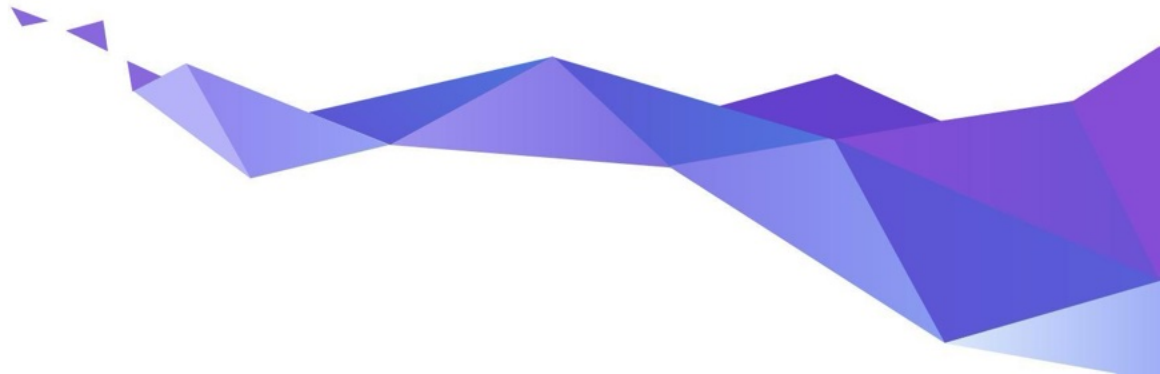


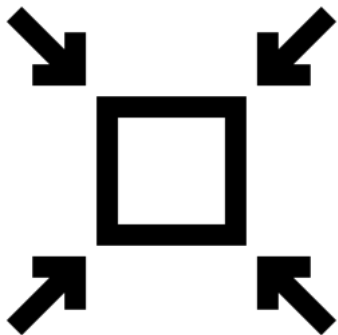
# Zephyr Project Overview

A proven RTOS ecosystem, by developers, for developers



# Use cases for a real-time OS



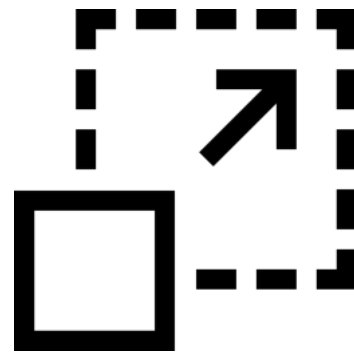


**SMALL**

< 8KB Flash

< 5KB RAM

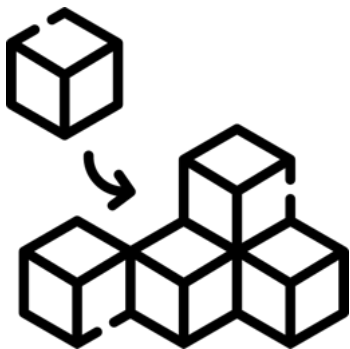
*yet*



**SCALABLE**

from small sensor nodes

... to complex multi-core systems



# FLEXIBLE

Heavily customizable

Out-of-the-box support for  
600+ boards and 100s of sensors

*yet*



# SECURE

Built with safety & security in mind

Certification-ready  
Long-term Support

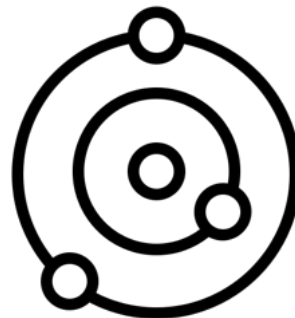




# OPEN-SOURCE

Permissively licensed (Apache 2.0)

Vendor-neutral governance



# ECOSYSTEM

Vibrant community

Supported by major silicon vendors

# Features overview

- **Lightweight kernel & supporting drivers and services**
- **Portable, secure, power-efficient**
- **Highly connected**
  - Bluetooth 5.0 & BLE
  - Wi-Fi, Ethernet, CANbus, ...
  - IoT protocols: CoAP, LwM2M, MQTT, OpenThread, ...
  - USB & USB-C
- **Complete developer environment**
  - Toolchain and HAL management
  - Emulation/Simulation
  - Logging, tracing, debugging,
  - Testing framework



# Products Running Zephyr Today



Otonon More  
Hearing Aid



Lildog & Lilcat  
Pet Tracker



Livestock Tracker



Moto Watch 100



Samsung Galaxy  
Ring



Proglove



Adhoc Smart Waste



Google  
Chromebook



Framework laptop



Keeb.io BDN9



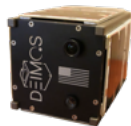
Hati-ACE



Safety Pod



BLiXT solid state  
circuit breaker



Aethero Deimos  
Satellite



PHYTEC Distancer



Laird Connectivity  
sensors & gateways



BeST pump  
monitoring



Vestas Wind  
Turbines

 [zephyrproject.org/products-running-zephyr](https://zephyrproject.org/products-running-zephyr)

# Products Running Zephyr Today



Discreet rechargeable hearing aid that gives you access to all relevant sounds

Oticon More supports the brain in making sense of sound and it is easy to operate with a double push button for volume and programme control. It features Bluetooth wireless technology for seamless connectivity with your favourite devices.

**oticon**  
life-changing **technology**

Bluetooth LE

Low Power



[zephyrproject.org/portfolio/oticon-more](https://zephyrproject.org/portfolio/oticon-more)

# Products Running Zephyr Today



## Sustainable energy solutions

Vestas is the energy industry's global partner on sustainable energy solutions. We design, manufacture, install, and service onshore and offshore wind turbines across the globe, and with more than 164 GW of wind turbines in 87 countries, we have installed more wind power than anyone else. Through our industry-leading smart data capabilities and unparalleled more than 144 GW of wind turbines under service, we use data to interpret, forecast, and exploit wind resources and deliver best-in-class wind power solutions. Together with our customers, Vestas' more than 28,000 employees are bringing the world sustainable energy solutions to power a bright future.

***Vestas***®

CANbus

Industrial Control



[zephyrproject.org/portfolio/vestas-wind-turbines](https://zephyrproject.org/portfolio/vestas-wind-turbines)

# Products Running Zephyr Today



## Thin, light, high-performance 13.5" notebook

A thin, light, high-performance 13.5" notebook that is also easy to repair, upgrade, and customize. The embedded controller firmware is a fork of the Zephyr version of chromium-ec, and is fully open source.



Embedded Controller

USB / USB-C

Power Mgmt



[zephyrproject.org/portfolio/framework-laptop-13-diy-edition-amd-ryzen-7040-series](https://zephyrproject.org/portfolio/framework-laptop-13-diy-edition-amd-ryzen-7040-series)

# Products Running Zephyr Today



## Professional grade, digital tape measure

The T1 Tomahawk, the world's first, professional grade, digital tape measure enables tradespeople, across industries, to collect measurements faster and more accurately than ever before. A live view, OLED display, shows measurements of the tape measure, digitally, in both english and metric units. With a click of a button, measurements are saved to a side mounted e-paper display as well as sent over Bluetooth to connected devices.



Low Power

Sensing



[zephyrproject.org/portfolio/reekon-t1-tomahawk](https://zephyrproject.org/portfolio/reekon-t1-tomahawk)



# Products Running Zephyr Today



Turns your wired sensors into IP67-rated battery-operated wireless nodes, providing robust and secure messaging

Ezurio's Sentries™ BT610 I/O Sensor with Bluetooth 5 turns your wired sensors into IP67-rated battery-operated wireless nodes, providing robust and secure messaging. Leveraging our BL654 module, it provides full Bluetooth 5 capabilities, opening up industrial and equipment monitoring applications.



Bluetooth

Cellular

Connectivity Management

App Framework



[zephyrproject.org/portfolio/sentries](https://zephyrproject.org/portfolio/sentries)



# 750+ supported boards... and growing



Arduino Portenta  
H7



ESP32



Sipeed HiFive1



nRF9160 DK



STM32F746G Disco



M5StickC PLUS



TDK RoboKit 1



BBC micro:bit 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



[docs.zephyrproject.org/latest/boards/](https://docs.zephyrproject.org/latest/boards/)

# 220+ Sensors Already Integrated



adt7420  
adx1345  
adx1362  
adx1372  
ak8975  
amg88xx  
ams\_as5600  
ams\_iAQcore  
apds9960  
bma280  
bmc150\_magn  
bme280  
bme680  
bmg160  
bmi160  
bmi270  
bmm150  
bmp388  
bq274xx  
ccs811

dht  
dps310  
ds18b20  
ens  
esp8266  
fdc3v3  
fxos8700  
fxos9700  
grove  
grow\_r502a  
hmc58831  
hp206c  
ht221  
i2c50c  
i2c605  
i2c670  
i2c720  
icp1125  
iis2dh  
iis2dlpc



iis2iclx  
iis2mdc  
iis3dhhc  
ina219  
ina230  
isl2935  
ism330dxx  
ite\_tach\_it8xxx2  
ite\_vcmp\_it8xxx2  
lis2dh  
lis2ds12  
lis2dw12  
lis2n  
lis3n  
lm75  
lm77  
lps22  
lps22hh  
lps25hb  
lsm303dlhc\_magn



lsm6ds0  
lsm6dsl  
lsm6dsx  
lsm9ds0  
lsm9ds0\_mfd  
max17055  
max17262  
max30101  
max31875  
max44009  
max6675  
mchp\_tach\_xec  
mcp9804  
mcp9808  
mcp9810  
mcp9812  
mcp9814  
mcp9816  
mcp9818  
mcp9820  
mcp9822  
mcp9824  
mcp9826  
mcp9828  
mcp9830  
mcp9832  
mcp9834  
mcp9836  
mcp9838  
mcp9840  
mcp9842  
mcp9844  
mcp9846  
mcp9848  
mcp9850  
mcp9852  
mcp9854  
mcp9856  
mcp9858  
mcp9860  
mcp9862  
mcp9864  
mcp9866  
mcp9868  
mcp9870  
mcp9872  
mcp9874  
mcp9876  
mcp9878  
mcp9880  
mcp9882  
mcp9884  
mcp9886  
mcp9888  
mcp9890  
mcp9892  
mcp9894  
mcp9896  
mcp9898  
mcp9900  
mcp9902  
mcp9904  
mcp9906  
mcp9908  
mcp9910  
mcp9912  
mcp9914  
mcp9916  
mcp9918  
mcp9920  
mcp9922  
mcp9924  
mcp9926  
mcp9928  
mcp9930  
mcp9932  
mcp9934  
mcp9936  
mcp9938  
mcp9940  
mcp9942  
mcp9944  
mcp9946  
mcp9948  
mcp9950  
mcp9952  
mcp9954  
mcp9956  
mcp9958  
mcp9960  
mcp9962  
mcp9964  
mcp9966  
mcp9968  
mcp9970  
mcp9972  
mcp9974  
mcp9976  
mcp9978  
mcp9980  
mcp9982  
mcp9984  
mcp9986  
mcp9988  
mcp9990  
mcp9992  
mcp9994  
mcp9996  
mcp9998  
mcp10000



nrf5  
nuvoton\_adc\_cmp\_npcx  
nuvoton\_tach\_npcx  
nxp\_kin  
opt3001  
pcnt\_encoder3  
pms7003  
qdec\_mcp  
qdec\_nrfx  
qdec\_sam  
qdec\_stm32  
rpi\_pico\_temp  
sbs\_gaug  
sgp40  
sht3xd  
sht4x  
shtcx  
si7006  
si7055  
si7060



si7210  
sm3511t  
stm32\_temp  
stm32\_vbat  
stmemsc  
stts751  
sx9500  
th02  
ti\_hdc  
ti\_hdc20xx  
tmp007  
tmp108  
tmp112  
tmp116  
vcnl4040  
vl53l0x  
wsen\_hids  
wsen\_itds

 [github.com/zephyrproject-rtos/zephyr/tree/main/drivers/sensor](https://github.com/zephyrproject-rtos/zephyr/tree/main/drivers/sensor)

# Supported Hardware Architectures



Cortex-M, Cortex-R  
& Cortex-A

x86 & x86\_64



32 & 64 bit

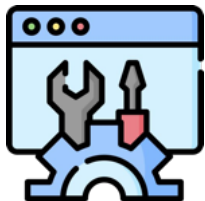


Xtensa



[docs.zephyrproject.org/latest/hardware/index.html#hardware-support](https://docs.zephyrproject.org/latest/hardware/index.html#hardware-support)

# Vibrant Ecosystem



**Development Tools**



**Zephyr<sup>®</sup>**

Governing Board

Technical Steering Committee

Contributors



**Applications & Middlewares**

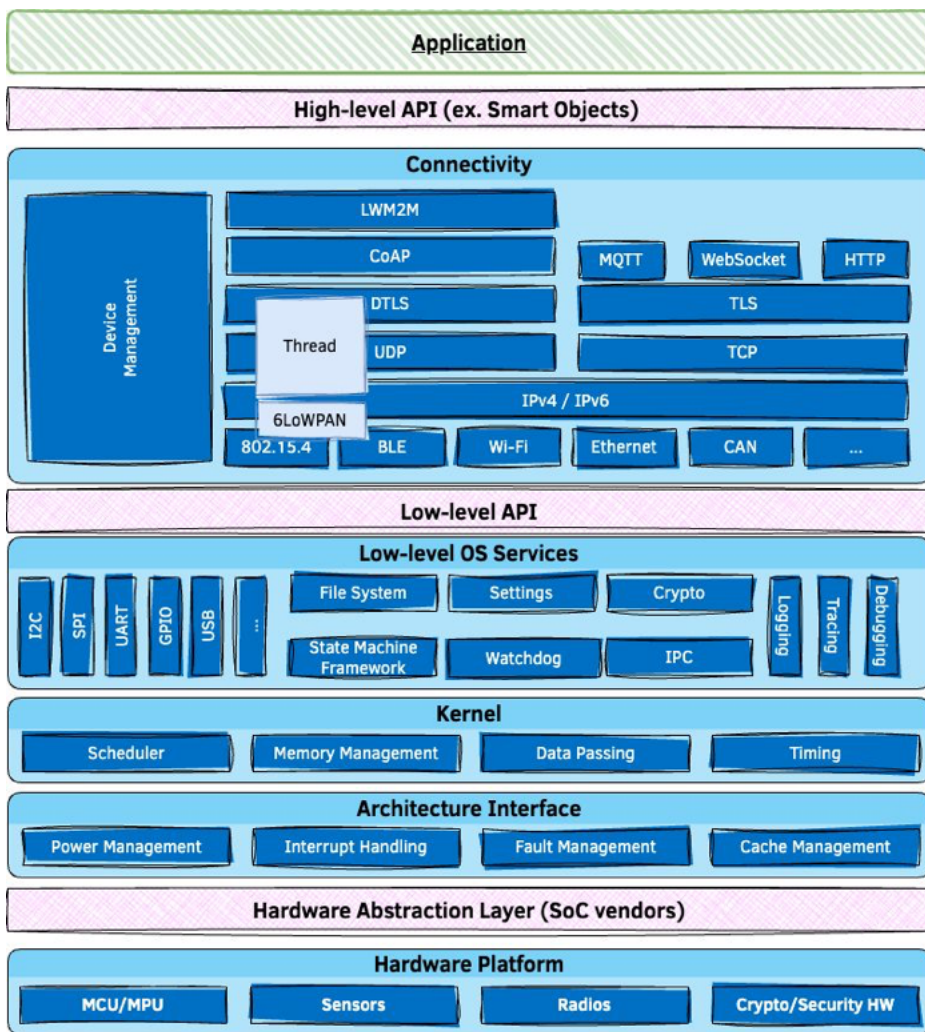


**Training & Consulting**

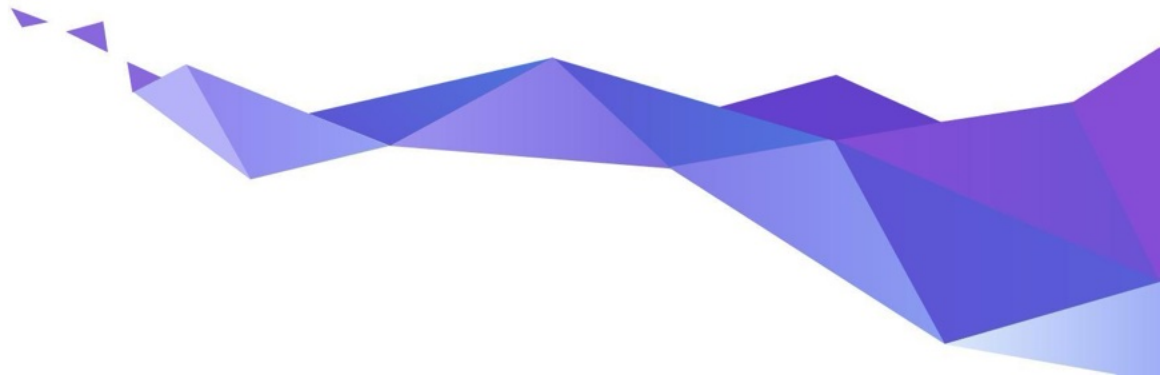


**Firmwares & Libraries**

# Architecture



# Diving into Zephyr's features



# Devicetree

**Describe & configure** the available hardware on the target system

**Decouple** the application from the hardware

+ **Kconfig** for all things configuration



[docs.zephyrproject.org/latest/build/dts](https://docs.zephyrproject.org/latest/build/dts)

```
&i2c1 {
    pinctrl-0 = <&i2c1_scl_pb8 &i2c1_sda_pb9>;
    pinctrl-names = "default";
    clock-frequency = <I2C_BITRATE_FAST>;
    status = "okay";

    lsm6dsl@6a {
        compatible = "st,lsm6dsl";
        reg = <0x06a >;
    };

    hts221@5f {
        compatible = "st,hts221";
        reg = <0x5f >;
    };

    // ...
};
```

.dts file example

# West meta-tool



- **Module Management**

- Simplifies Versioning and integration of various modules/libraries in the build system

- **Build**

- **Extensible `command-line interface`**

- e.g. custom commands for specific board
- Static code analysis, RAM/ROM reports



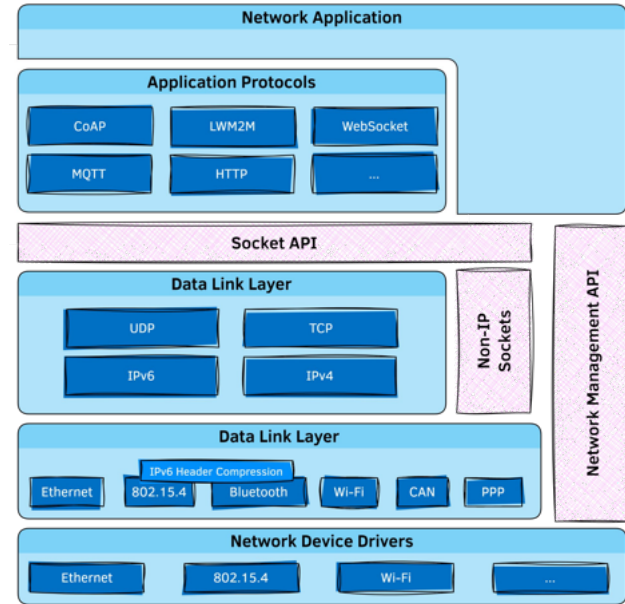
# Connectivity Options

- 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 5.3 compliant •  
LE Controller • Host • Mesh •  
Bluetooth-SIG qualifiable



USB 2.0 • USB-C •  
Device & Host • WebUSB

# 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

# Devicetree



**Describe & configure** the available hardware on the target system

**Decouple** the application from the hardware



[docs.zephyrproject.org/latest/build/dts](https://docs.zephyrproject.org/latest/build/dts)

```
&i2c1 {
    pinctrl-0 = <&i2c1_scl_pb8 &i2c1_sda_pb9>;
    pinctrl-names = "default";
    clock-frequency = <I2C_BITRATE_FAST>;
    status = "okay";

    lsm6dsl@6a {
        compatible = "st,lsm6dsl";
        reg = <0x06a >;
    };

    hts221@5f {
        compatible = "st,hts221";
        reg = <0x5f >;
    };

    // ...
};
```

.dts file example

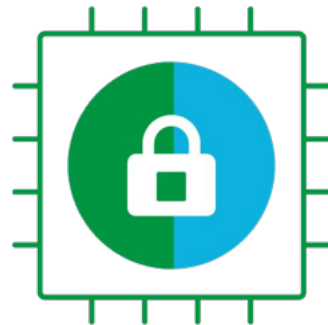
# Secure boot / Device Management



- 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

- **Cryptography APIs**
  - 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 $\mu$ s
Thread start	3.6 $\mu$ s
Thread suspend	3.3 $\mu$ s
Thread resume	3.8 $\mu$ s
Context switch (yield)	2.2 $\mu$ s
Get semaphore	0.6 $\mu$ s
Put semaphore	1.1 $\mu$ s

# 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



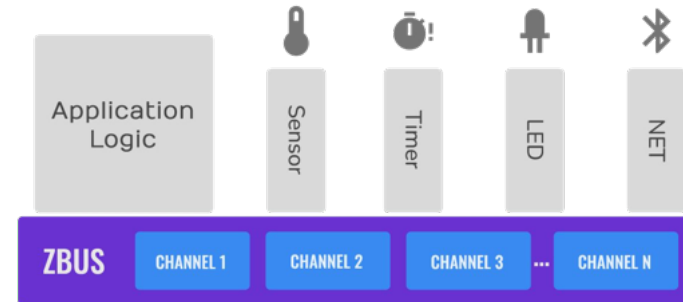
# Inter-Process Communication



- **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
Pipe	✗	Ring buffer

*Data passing objects available in Zephyr kernel*

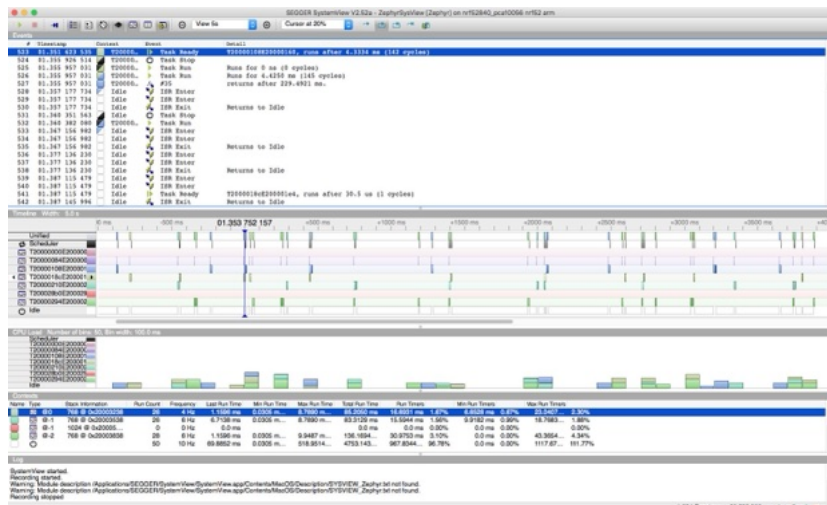


*A typical zbus application architecture*

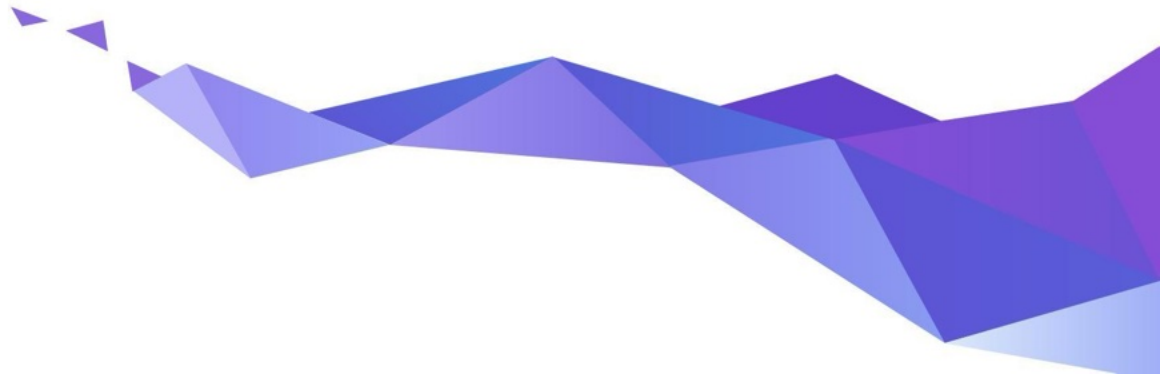
# Tracing & Debugging



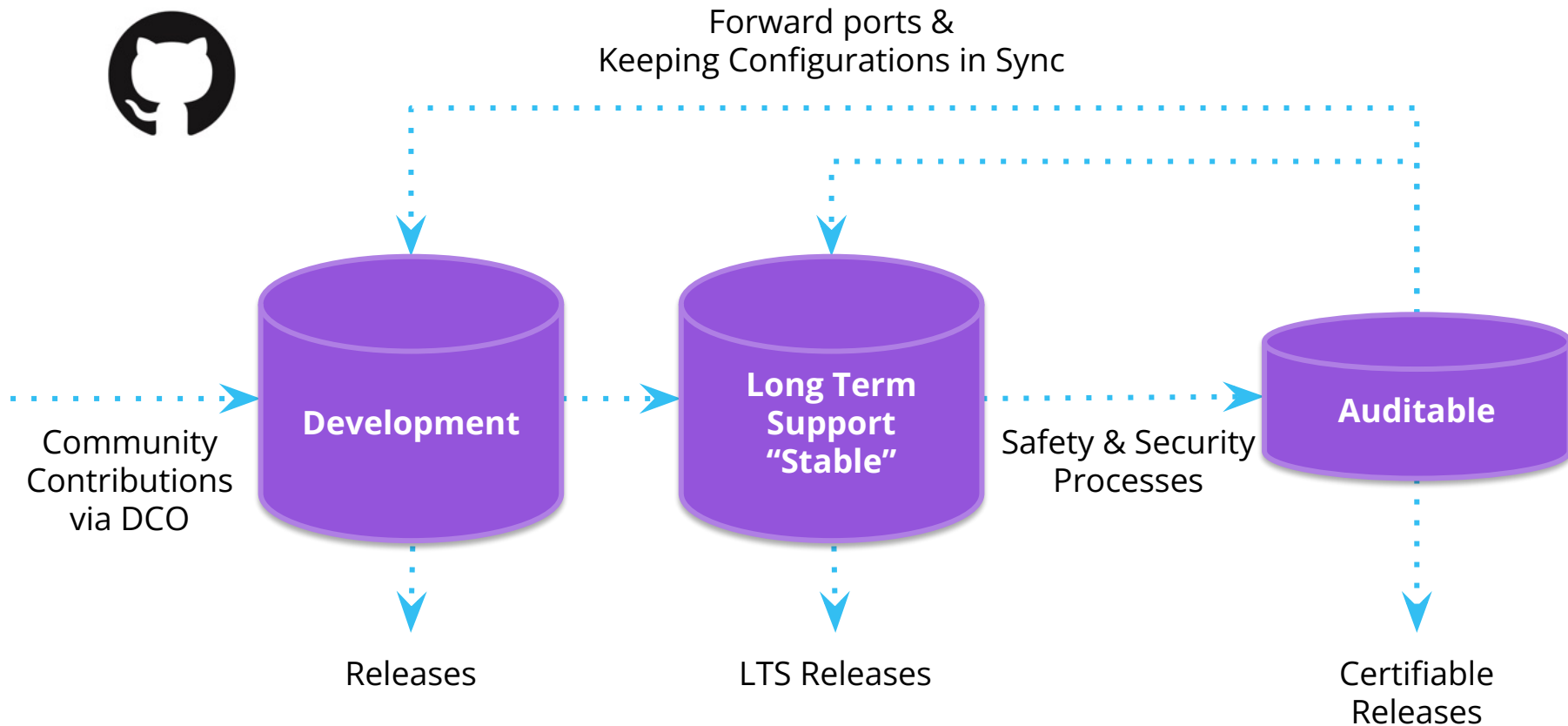
- Advanced **logging** framework
  - Multiple backends (UART, network, file system, ...)
  - Compile-time & runtime filtering
- **Tracing** framework
  - Visualize the inner-working of the kernel and its various subsystems
  - Object tracking (mutexes, timers, etc.)



# Safety & 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
- **Supported for 2+ years**
-  **Doesn't include cutting-edge functionality**



[github.com/zephyrproject-rtos/zephyr/releases/tag/zephyr-v2.7.0](https://github.com/zephyrproject-rtos/zephyr/releases/tag/zephyr-v2.7.0)



# Long Term Support (LTS - 1.14)



The image displays a collage of four GitHub release pages for the Zephyr project, illustrating its Long Term Support (LTS) for version 1.14. The pages are:

- Zephyr 1.14.0:** Announced on April 16, 2020. Major enhancements include support for 160 different board configurations, a reworked and reimplemented timing subsystem, and a new CPU affinity API.
- Zephyr 1.14.1:** An LTS maintenance release from November 2020. It includes security vulnerability fixes, Bluetooth qualification listings, and various bug fixes related to the Bluetooth BR/EDR specification and host subsystem.
- Zephyr LTS 1.14.2 (Maintenance Release):** Released in December 2020. It addresses security vulnerabilities (CVEs) and issues fixed since the previous 1.14.0 tagged release.
- Zephyr v1.14.3:** Released in January 2021. It continues the LTS maintenance, addressing security vulnerabilities and issues fixed since the previous 1.14.0 tagged release.

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](#) [Report an issue with this page](#)

This is the documentation for the latest (main) development branch of Zephyr. If you are looking for the documentation of previous releases, use the dropdown 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:

1. **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

# Software Supply Chain



- 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  
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libkernel.a  
[...]
```

# Automating SBOM Generation During Build!



1. Create a build directory with CMake file API enabled
2. Build project with “build metadata” enabled
3. Compute SBOM(s)

```
west spdx --init -d BUILD_DIR
west build -d BUILD_DIR -- -DCONFIG_BUILD_OUTPUT_META=y
west spdx -d BUILD_DIR
```



- |                    |   |
|--------------------|---|
| <b>zephyr.spdx</b> | SBOM for the <b>Zephyr source files</b> actually used by your application |
| <b>app.spdx</b>    | SBOM for the source files of your <b>application</b>                      |
| <b>build.spdx</b>  | SBOM for <b>all the build objects</b> , inc. of course your final image   |

# SBOM's at Scale...Automatically



708 boards

13 apps

**All BUILT,  
PASSED,  
GENERATED**  
have **3 SBOMs**  
available to  
download &  
inspect

A screenshot of the Zephyr Dashboard web interface. The browser address bar shows "zephyr-dashboard.renode.io". The page features a search bar, a navigation menu on the left with "ARCHITECTURE" and "BUILD DETAILS" sections, and a main content area displaying a table of boards. The table has columns for board names and their build status across five different categories. The status indicators are color-coded: green for "PASSED", orange for "GENERATED", and blue for "BUILT". A "Download SBOM" button is visible in the interface.

BOARD NAME	HELLO WORLD	PHILOSOPHERS	SHELL MODULE	TENSORFLOW LITE MICRO	MICROPYTHON
ARC (20) ^					
ARM32 (529) ^					
ARM64 (26) ^					
MIPS (2) ^					
NIOS2 (2) ^					
RISCV32 (35) v					
Andes ADP-XC7K AE350	PASSED	GENERATED	PASSED	Download SBOM	PASSED
ESP32-C3	BUILT	BUILT	BUILT	BUILT	BUILT
ESP32C3 LuatOS Core	BUILT	BUILT	BUILT	BUILT	BUILT
ESP32C3 LuatOS Core USB	BUILT	BUILT	BUILT	BUILT	BUILT
GigaDevice GD32VF103C-STARTER	GENERATED	GENERATED	GENERATED	GENERATED	NOT BUILT
GigaDevice GD32VF103V-EVAL	GENERATED	GENERATED	GENERATED	GENERATED	GENERATED
ICE-V Wireless	BUILT	BUILT	BUILT	BUILT	BUILT

Source: <https://zephyr-dashboard.renode.io/>

# CVE Numbering Authority



- [Registered with MITRE](#)  
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 <a href="#">↗</a> ; 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	<a href="#">MITRE Corporation</a>
Security Advisories	<a href="#">View Advisories</a>
Program Role	CNA
Organization Type	Vendors and Projects
Country*	USA

# OpenSSF 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
- Gold status since Feb, 2019



## Zephyr Project

[Expand 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**
- The project aims at **fixing issues within 30 days** to give **vendors 60 days** before publication of vulnerability

A screenshot of the Zephyr Project's Product Creators Vulnerability Alert Registry form. The page has a blue header with the Zephyr logo and navigation links. The main content area is white with a blue gradient background at the top. The form includes a title, a brief introduction, a list of participation criteria, a disclaimer, and a series of input fields for personal and company information. At the bottom, there is a checkbox for consent and a "Submit" button. The footer contains social media icons and copyright information.

Product Creators Vulnerability Alert Registry

If you believe your organization meets the criteria to be eligible to receive vulnerability alerts please fill out the form below.

**Criteria for Participation**

- Have a product that will be exposed to a public audience and professionals how Zephyr is being used in the product.
- Have a publicly shared product feature on your website of Zephyr.
- Have an active membership in our mailing list.
- Accept the Zephyr Embargo Policy that is outlined below.

• Removal: If a member stops adhering to these criteria after joining the list then the member will be unenrolled.

More information on Zephyr's Security and Disclosure practices can be found at [Security](#).

First name\*  
Last name\*  
Email\*  
Phone number  
Company name\*  
Job title\*  
Link to your Company's Product that is built with Zephyr SDK. (e.g. <https://www.zephyrproject.org/>)  
Zephyr release in use\*  
Zephyr Embargo Policy  
The information members receive during embargo periods may be received on vulnerability announcements/embargos only. Any information regarding embargoed vulnerabilities must not be made public, shared, nor even listed on a private board beyond the needs to know within your specific team except with the team's explicit approval. This holds true until the public disclosure deadline that was agreed upon by the list members of the list and which may not use the information for anything other than getting the issue fixed for your respective product's users.  
Before any embargoed information is shared with respective members of your team required to be kept close, they must agree to the same terms and only that our information is a need to know basis.  
In the unfortunate event a member shares the information beyond what is allowed by this policy, that member must urgently inform the [subscribed@zephyrproject.org](#) mailing list of exactly what information leaked and to whom. A retrospective will take place after the leak so we can assess how to not make the same mistake in the future.  
If the member continues to leak information and break this policy, the member will be removed from the list.  
More details of how vulnerabilities are handled can be found in our [Security Policies & Processes](#) documentation.  
 I agree to receive other communications from The Linux Foundation.  
By submitting this form, I acknowledge that my information is subject to The Linux Foundation's [Privacy Policy](#).  
Submit

# Zephyr PSIRT: Remediation and Response



## 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.

**AMNESIA:33**  
Research Report Executive Summary

- **Foresecout Research Labs** has launched **Project Memoria**, an initiative 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 pose to the extended enterprise and how to mitigate those.
- **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 campaigns, such as botnets, without them being aware.

**150+**  
VENDORS AFFECTED

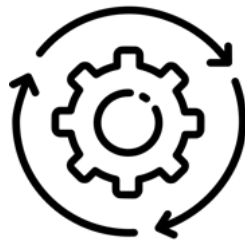
foresecout.com/amnesia33 | research@foresecout.com | tel: +1-866-377-8771

# Zephyr Security Summary



[Documented secure coding practices](#)

Vulnerability response criteria publicly documented

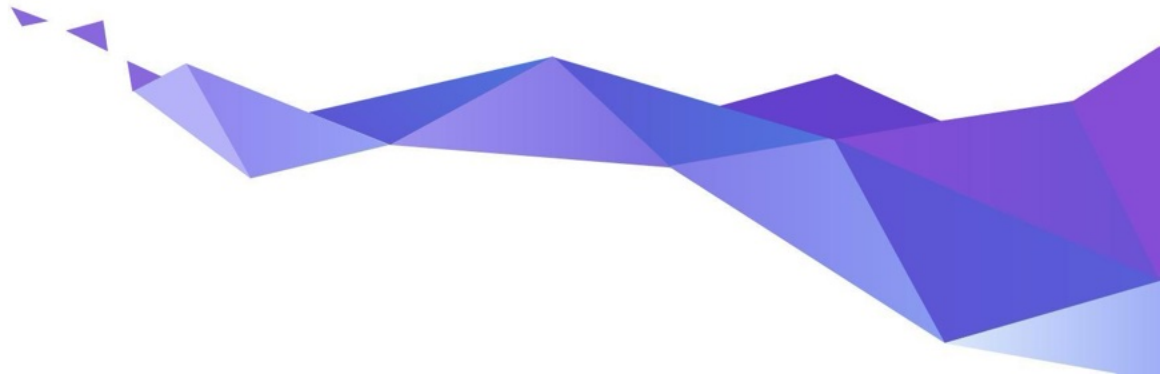


Weekly Coverity scans  
MISRA scans



SBOM generation

# Certification



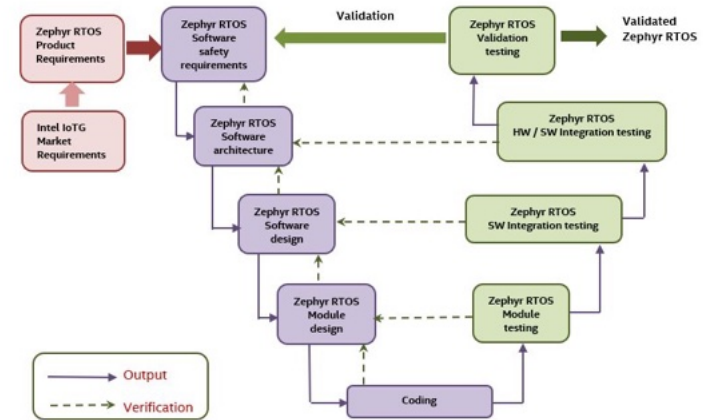
# Compliant Development: V-model



It is difficult to map a stereotypical open-source development to the V-model

- Specification of features
- Comprehensive documentation
- Traceability from requirements to source code
- Number of committers and information known about them

Zephyr RTOS functional safety work products mapping to IEC 61508-3 V model



⇒ Provide the evidences that open source developers can map to compliance and meet all requirements

# Safety Collateral Proposal



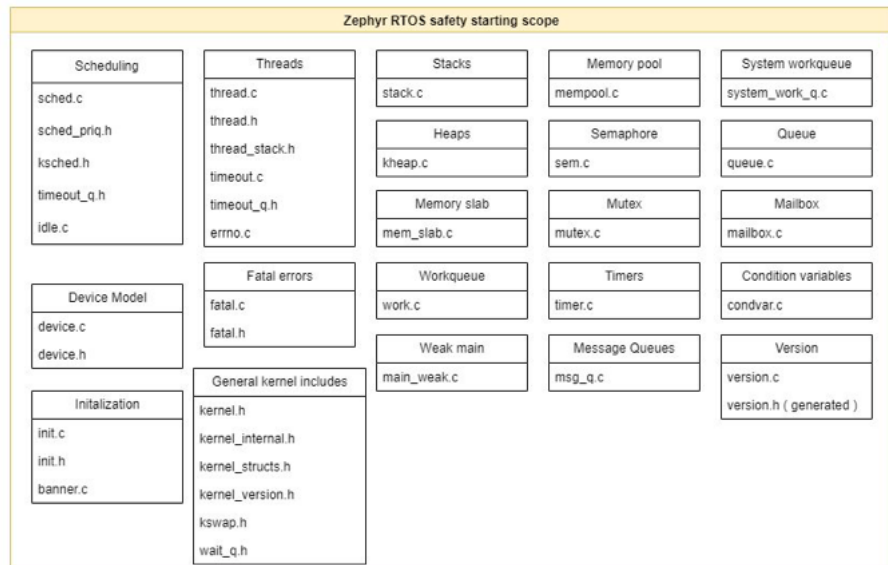
Draft (Pending Approval by Certification Authority)			
Artifacts	Type of Doc	Owner	Work in progress Visibility
<b>Plans</b>	Category		
Safety Development Plan	Plan/Process	Safety Committee	Public - Project Docs
Safety Assessment Plan	Plan/Process	FSM	Safety Committee Github
Verification / Validation / 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
<b>Specifications</b>	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
<b>Sources</b>	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
<b>Reports</b>	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
<b>Manuals</b>	Category		
Software User Manual	Manual	TSC	Public
Safety Manual	Manual	FSM	Safety Committee
<b>Certificates</b>			
All safety certificates	Certificate	Safety Committee	N/A

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

# Initial certification focus

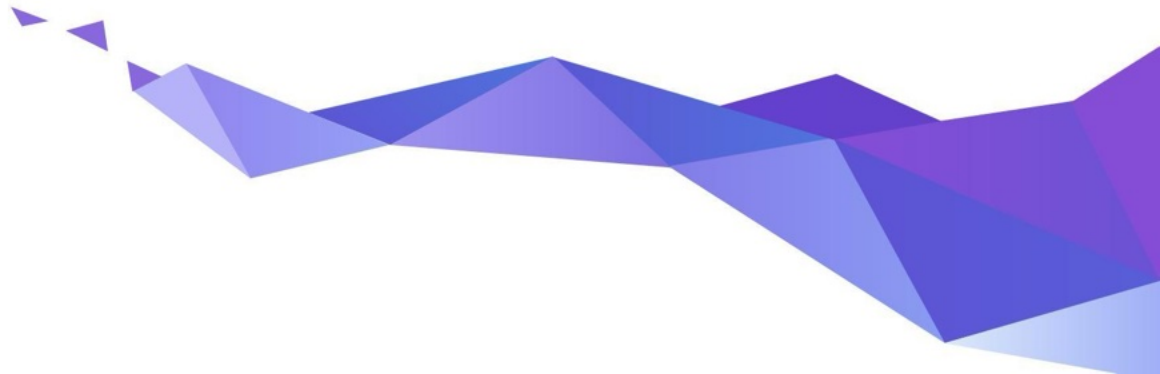


- Start with a limited scope of kernel and interfaces
- Initial target is IEC 61508 SIL 3 / SC 3 (IEC 61508-3, 7.4.2.12, Route 3s)
- Option for 26262 certification has been included in contract with certification authority should there be sufficient member interest



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

# Ecosystem & Governance





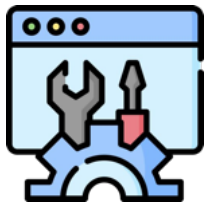
# Zephyr Project: Platinum Members



# Zephyr Project: Silver Members



# Vibrant Ecosystem



**Development Tools**



**Zephyr**<sup>®</sup>

Governing Board

Technical Steering Committee

Contributors



**Applications & Middlewares**



**Training & Consulting**



**Firmwares & Libraries**

# Ecosystem // Dev Tools



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

## IDE



## Compilers



## Debuggers / Tracing Tools



## Emulation / Simulation



# Ecosystem // Training & Consulting



## Training



## Services & Consulting



Development Tools



Training & Consulting

Firmwares & Libraries

Applications & Middlewares

# Ecosystem // Firmwares & Libraries



Development Tools



Training & Consulting

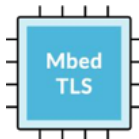


Firmwares & Libraries



Applications & Middlewares

## Security



## TinyML



## Language runtimes



## Others



# Ecosystem // Apps & Middlewares



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

## Remote Management



HERALD



Golioth



AVSYSTEM



Blynk



Memfault



STERNUM



blues

## Robotics



# Ecosystem // Developer Tools



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

## IDE



## Compilers



## Emulation / Simulation





# Ecosystem // Training & Consulting



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

## Training



## Services & Consulting



# Ecosystem // Firmwares & Libraries



Development Tools



Training & Consulting

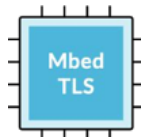


Firmwares & Libraries



Applications & Middlewares

## Security



## TinyML



## Language runtimes



## Others



# Ecosystem // Apps & Middlewares



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

## Remote Management



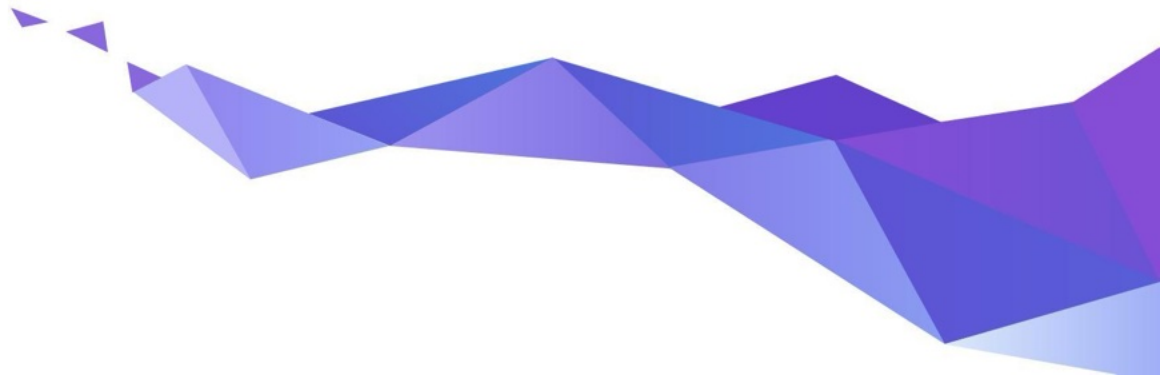
## Graphical Interfaces



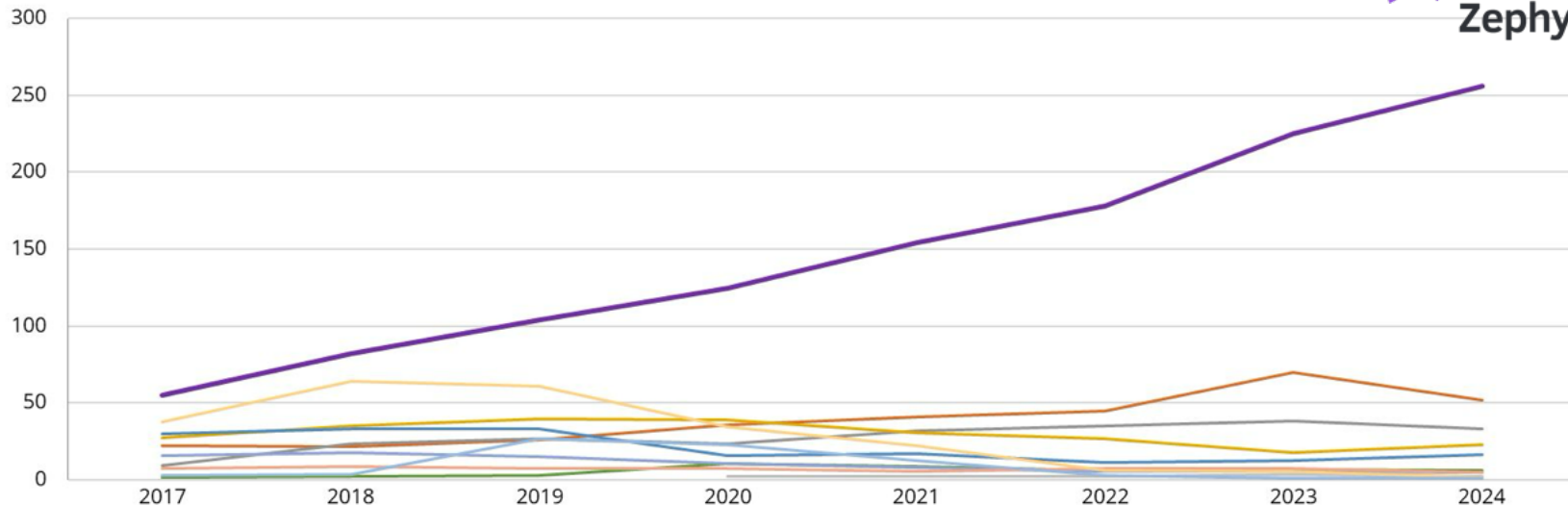
## Robotics



# Zephyr in the RTOS landscape

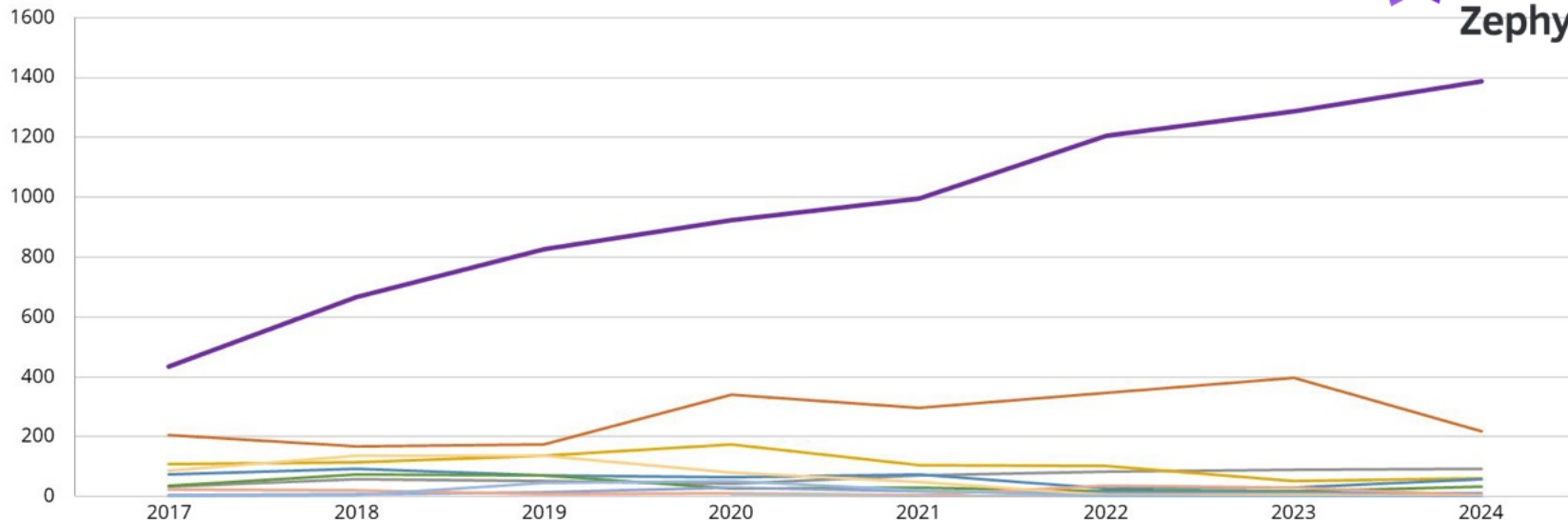


# Average Number of Unique Contributors per Month



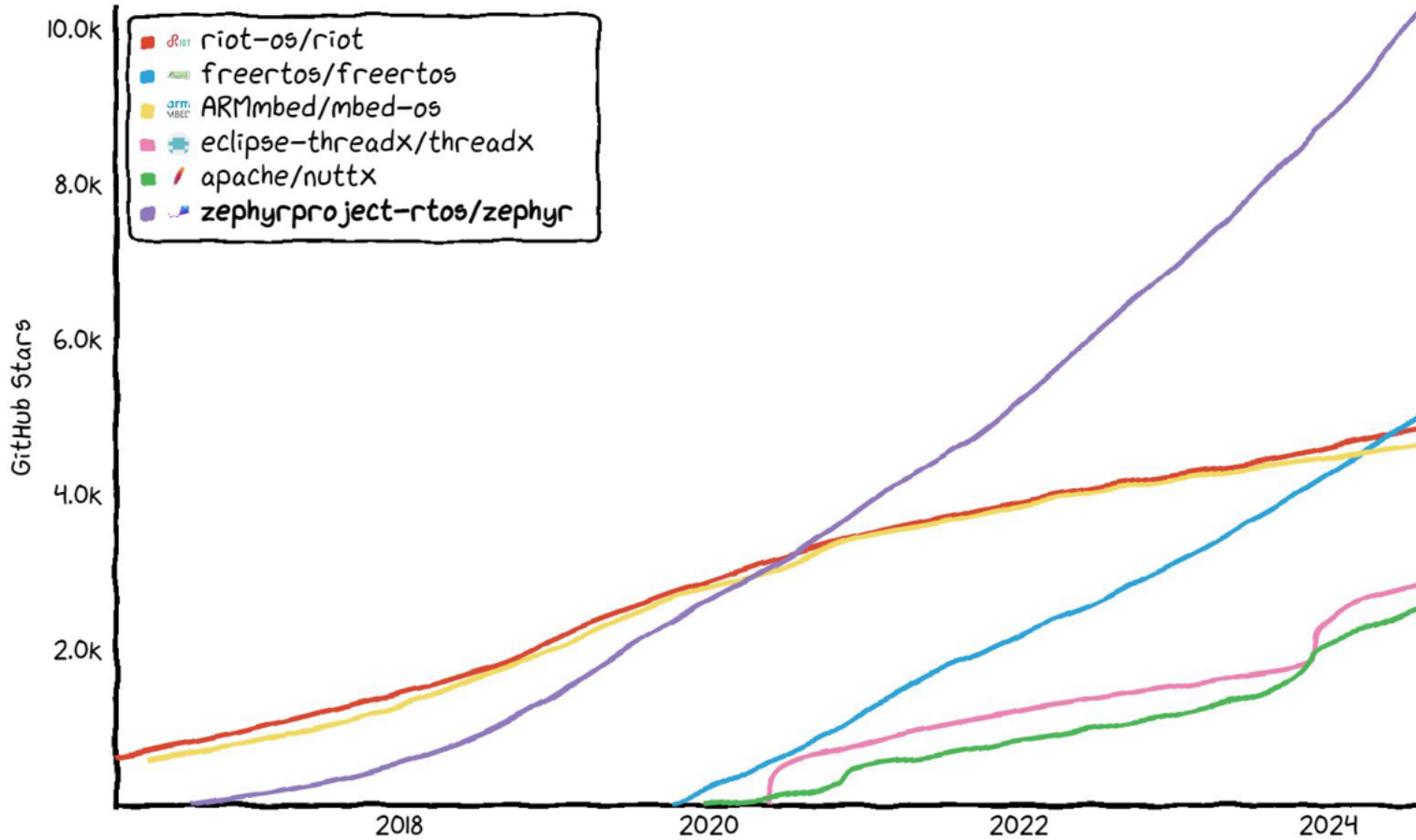
	2017	2018	2019	2020	2021	2022	2023	2024
Zephyr	55	82	104	125	154	178	225	256
Apache NuttX	22	22	26	36	41	45	70	52
RT-Thread	9	24	26	23	32	35	38	33
RIOT OS	27	35	39	39	30	27	18	23
TizenRT	30	33	33	15	17	11	13	16
FreeRTOS	2	2	3	11	8	6	7	6
Apache Mynewt	16	18	15	11	8	5	5	5
Contiki-NG	8	9	7	7	5	7	7	5
Eclipse ThreadX				2	2	2	3	2
Arm Mbed OS	38	64	61	35	22	6	5	2
Amazon FreeRTOS	3	3	27	23	13	3	1	1

# Average Number of Commits per Month

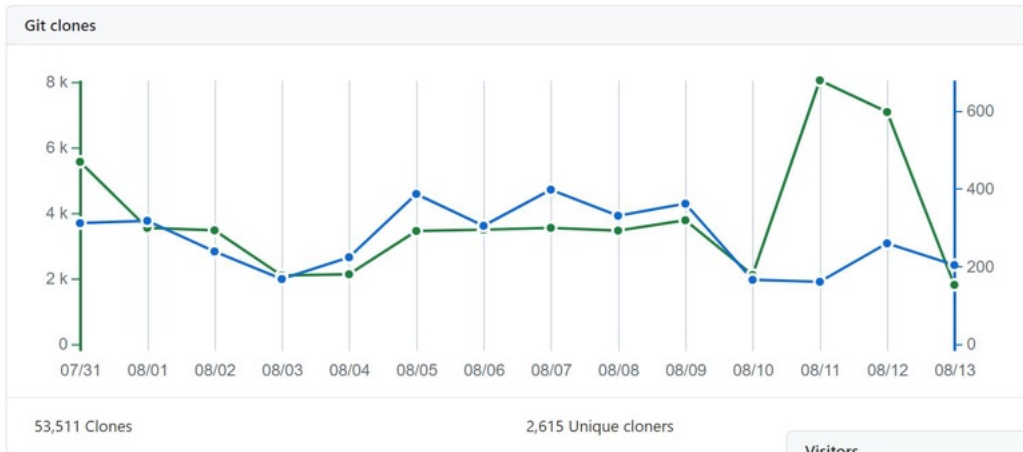


	2017	2018	2019	2020	2021	2022	2023	2024
Zephyr	434	667	825	924	995	1206	1287	1387
Apache NuttX	206	170	175	342	297	347	397	219
RT-Thread	35	59	53	43	70	84	91	92
RIOT OS	108	115	136	175	105	103	52	61
TizenRT	73	93	71	64	74	27	29	58
Apache Mynewt	38	74	70	27	31	18	19	33
FreeRTOS	4	8	13	32	17	11	12	11
Contiki-NG	23	22	9	11	7	38	30	6
Eclipse ThreadX				7	1	2	3	2
Arm Mbed OS	86	136	138	82	51	6	5	2
Amazon FreeRTOS	2	4	47	53	20	2	0	0

# Star History



# GitHub Clones & Unique Visitors



2024-07-31 → 2024-08-13

~186 unique clones per day  
~1375 unique visitors per day





# Getting started – Important links

- Check out the official [Getting Started Guide](#)
- Dig into the hundreds of **code samples**
- Check the catalog of 100s of available Devicetree bindings
  - No driver for your HW? Chances are a similar driver already exists and writing one is not as hard or daunting as you would think!
- Reach out to the community on **Discord**

# Zephyr Participation Information



[zephyrproject.org](https://zephyrproject.org)



[github.com/zephyrproject-rtos](https://github.com/zephyrproject-rtos)



[lists.zephyrproject.org](https://lists.zephyrproject.org)



[chat.zephyrproject.org](https://chat.zephyrproject.org)



[zephyrproject.org](https://zephyrproject.org)

