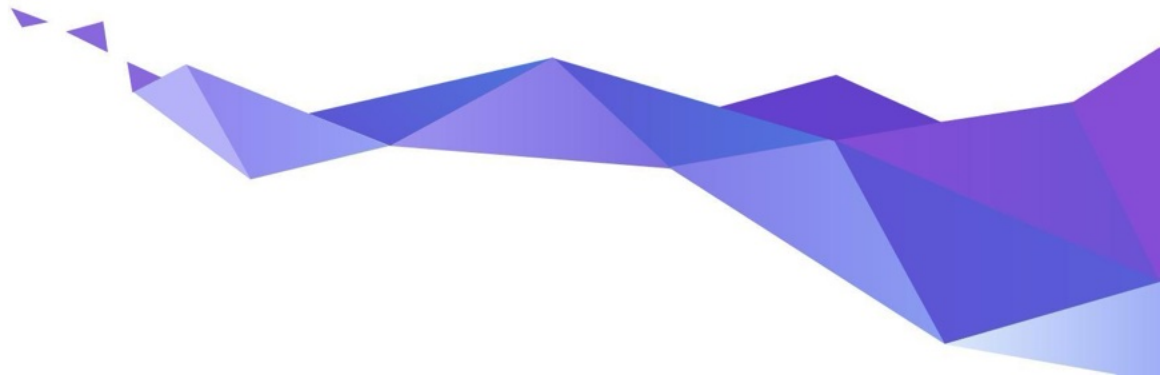


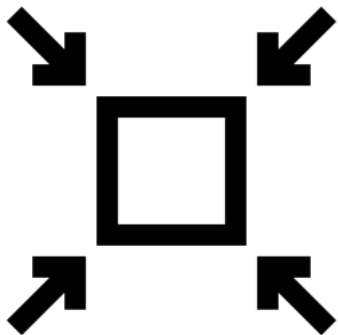
Zephyr Project Overview

A proven RTOS ecosystem, by developers, for developers



Use cases for a real-time OS



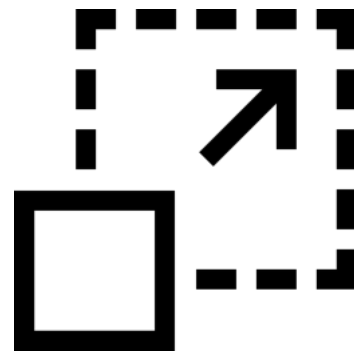


SMALL

< 8KB Flash

< 5KB RAM

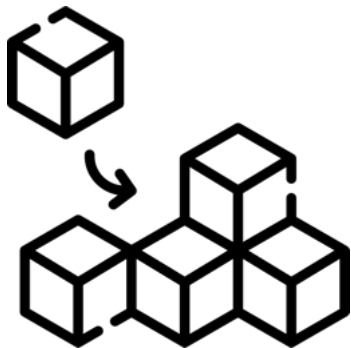
yet



SCALABLE

from small sensor nodes

... to complex multi-core systems



FLEXIBLE

Heavily customizable

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

yet



SECURE

Built with safety & security in mind

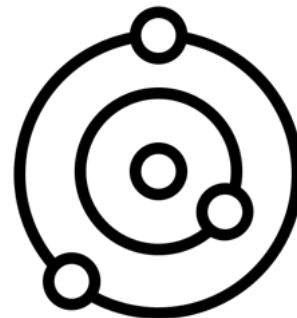
Certification-ready
Long-term Support



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



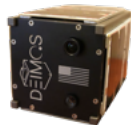
Hati-ACE



Blackhole™
PCIe AI Accelerator



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

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

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®

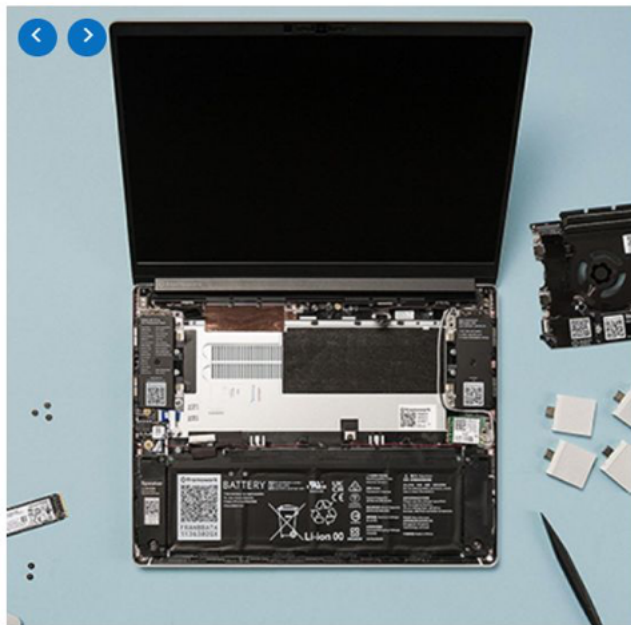
CANbus

Industrial Control



zephyrproject.org/portfolio/vestas-wind-turbines

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

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

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

1000+ supported boards...



Arduino Portenta
H7



ESP32



Sipeed HiFive1



nRF9160 DK



STM32F746G Disco



M5StickC PLUS



TDK RoboKit 1



BBC micro:bit v2



Blues Swan



Arduino Nano 33
BLE



Intel UP Squared



Dragino LSN50
LoRA Sensor Node



Quicklogic Qomu



Raspberry Pi Pico



Renesas RX130



NXP i.MX8MP EVK



Adafruit Feather
M0 LoRa



u-blox EVK-NINA-B3



docs.zephyrproject.org/latest/boards/

300+ 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
icp125
iis2dh
iis2dlpc



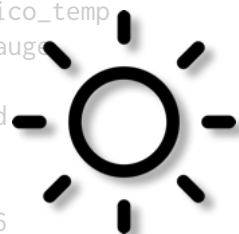
iis2iclx
iis2mdc
iis3dhhc
ina219
ina230
isl2935
ism330dxx
ite_tach_it8xxx2
ite_vcmp_it8xxx2
lis2dh
lis2ds12
lis2dw12
lis2n
lis3n
lm75
lm77
lps22
lps22hh
lps25hb
lsm303dlhc_magn



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
opt3000
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
stmesc
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

Supported Hardware Architectures



Cortex-M, Cortex-R
& Cortex-A

x86 & x86_64



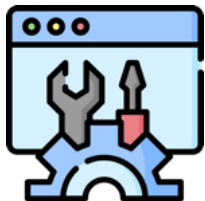
32 & 64 bit

Xtensa



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

Vibrant Ecosystem



Development Tools



Governing Board

Technical Steering Committee

Contributors



Applications & Middlewares

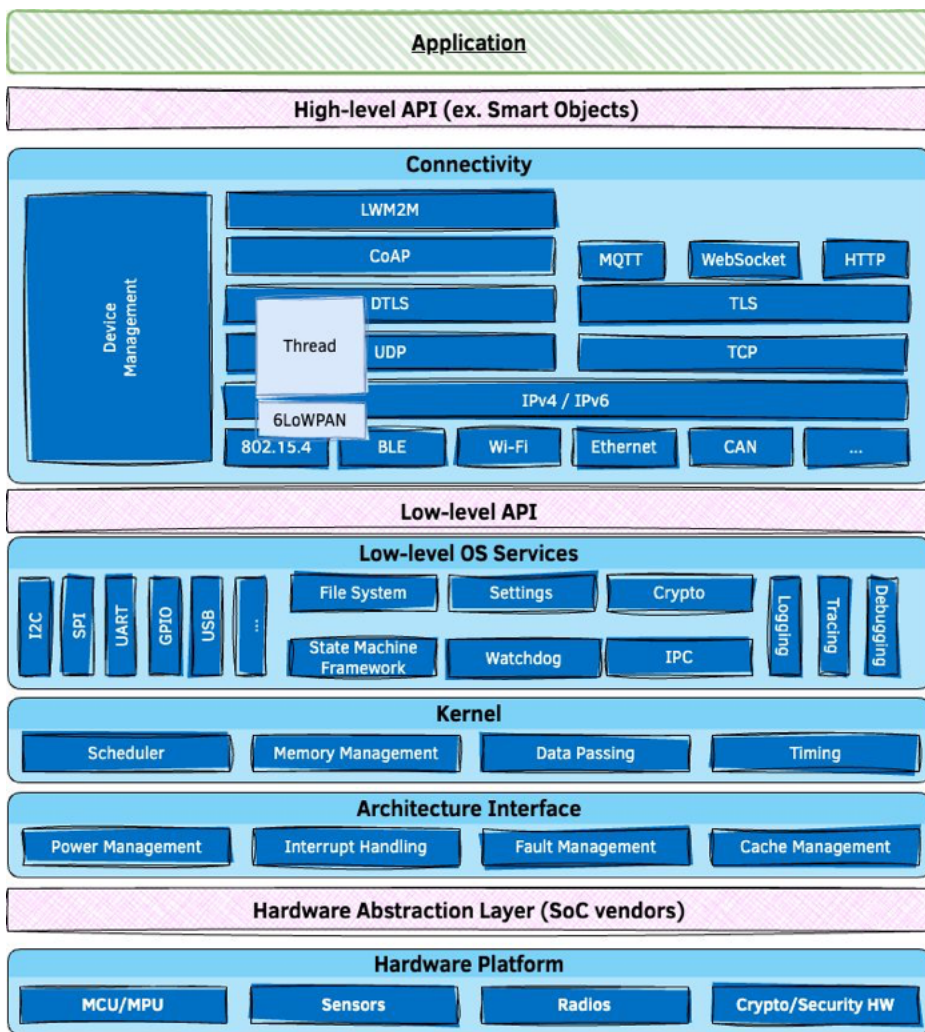


Training & Consulting

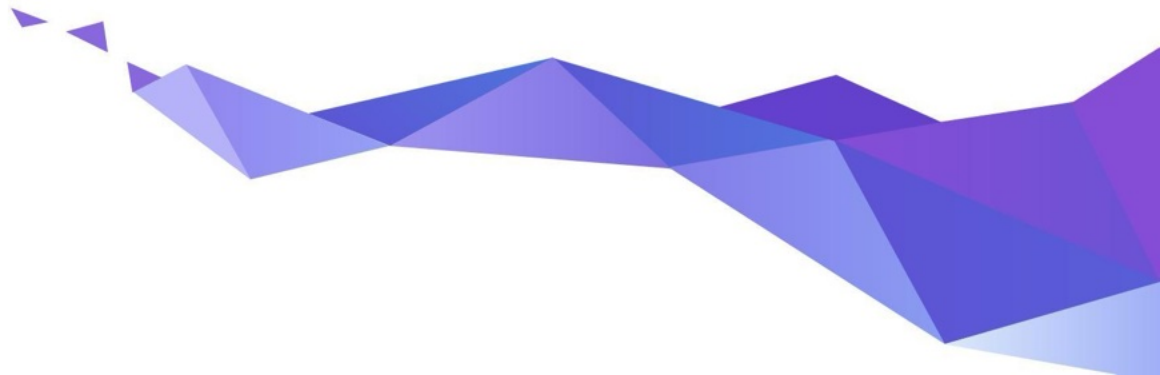


Firmwares & Libraries

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

```
&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

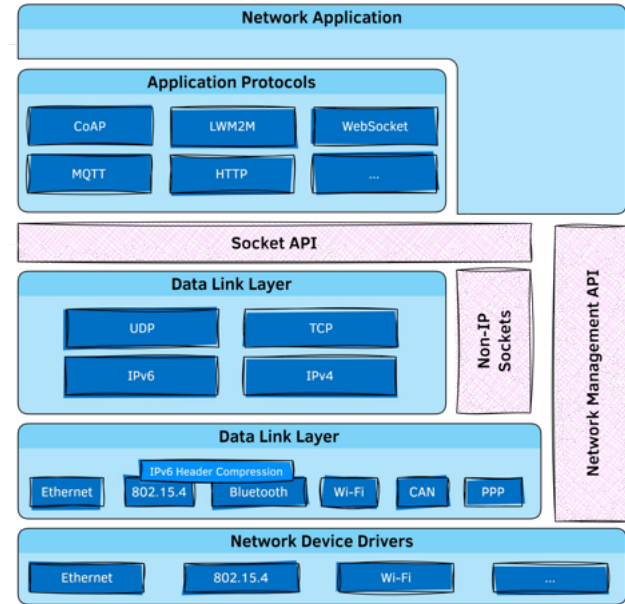
Connectivity Options

- 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** – MQTT (3.1.1, 5), CoAP and HTTP protocols
- **Over-the-air updates**
- **Device management** – 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, SNTTP
- 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**: reduce power consumption while preserving responsiveness
- **Key concepts**
 - **Tickless kernel**
 - System PM: idle thread, interruptions only for registered events
 - Device PM: device drivers can react to PM state changes
- Handled by the kernel / Customizable by the user
- Automated testing using Twister Power Harness

Devicetree

Describe & configure the available hardware on the target system

Decouple the application from the hardware



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

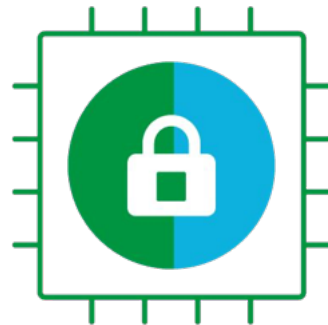
Secure boot / Device Management



- 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 μ s
Thread start	3.6 μ s
Thread suspend	3.3 μ s
Thread resume	3.8 μ s
Context switch (yield)	2.2 μ s
Get semaphore	0.6 μ s
Put semaphore	1.1 μ s

Graphical User Interfaces



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



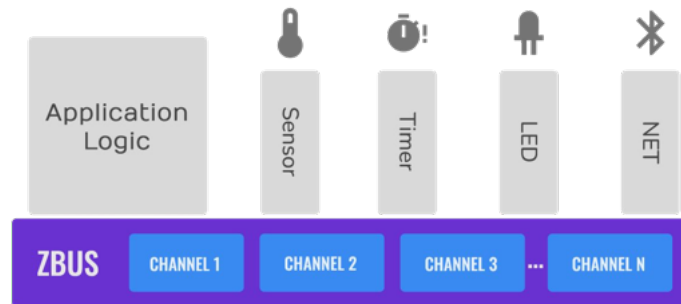
Inter-Process Communication



- **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

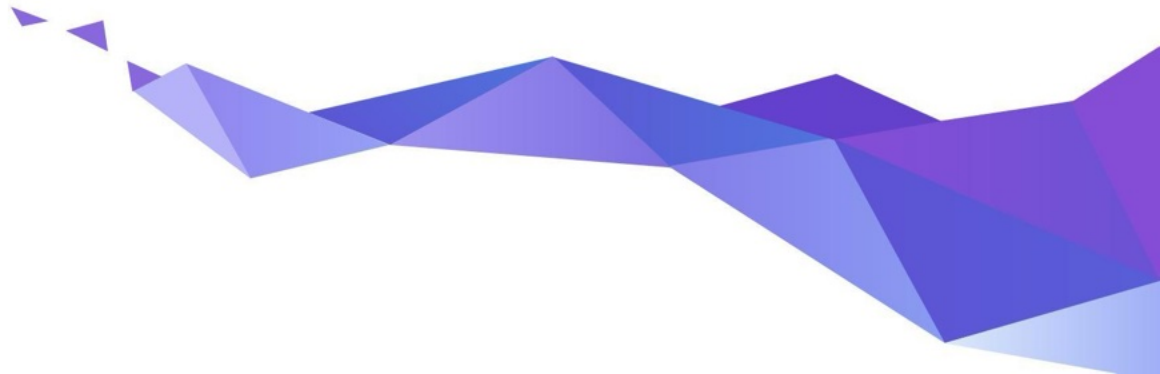
Zephyr 4.4 (Apr. 2026) – What's new?



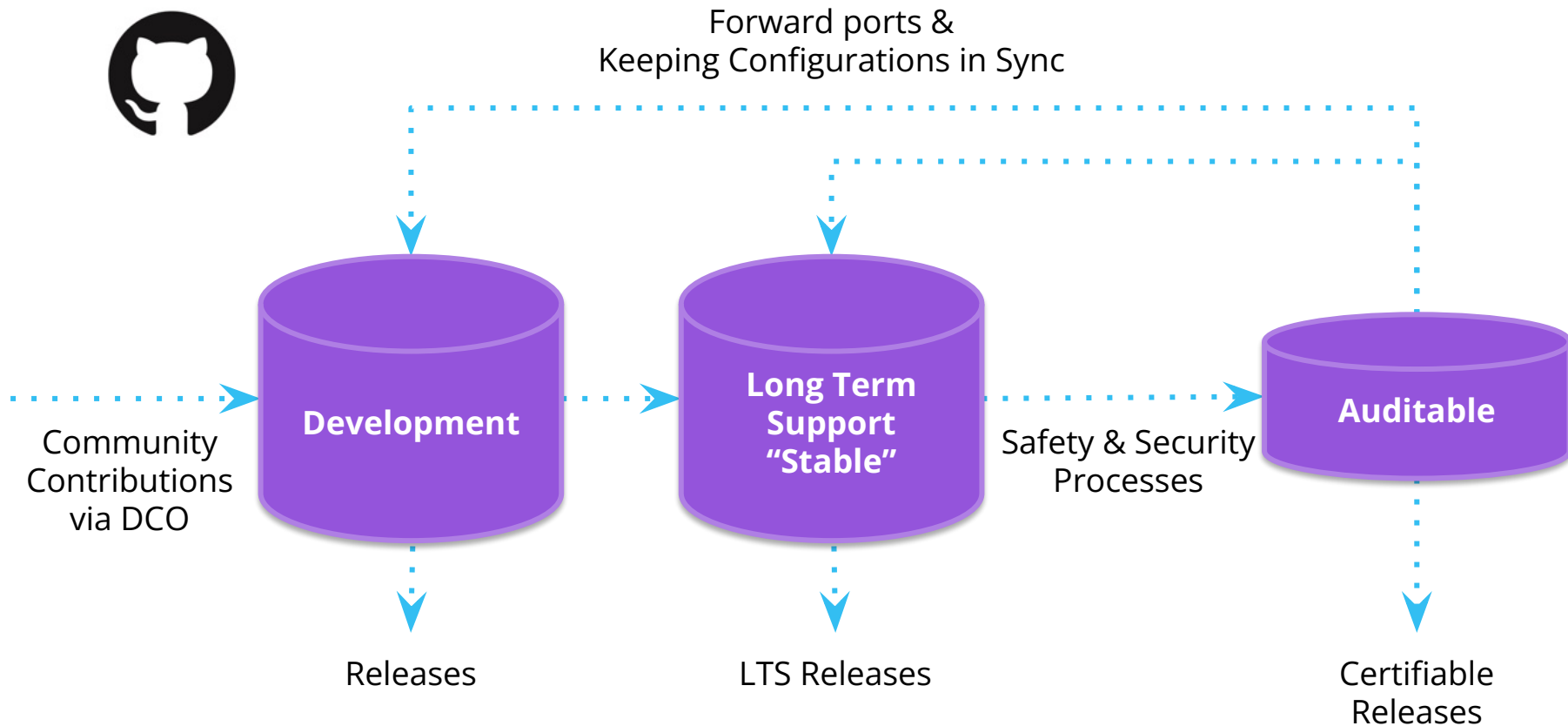
-  **Zephyr SDK 1.0** and support for **C17**
-  **Wireguard VPN**
-  **Wi-Fi Direct** for direct peer-to-peer communication over Wi-Fi
-  **USB Host** improvements, inc. USB Video Camera support
-  New driver classes: **Biometrics**, **One-Time Programmable memory**, **Wake-up Controllers**.
-  **Inter-domain zbus**

...and more! See [Release notes 4.4](#) & [Announcement blog post](#).

Safety & Security



Code Repositories



Long Term Support (Zephyr 3.7.x)



- **Product Focused**
- Current with latest **Security Updates**
- **Tested:** Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- **Supported for 5 years**
- **⚠ Doesn't include cutting-edge functionality**



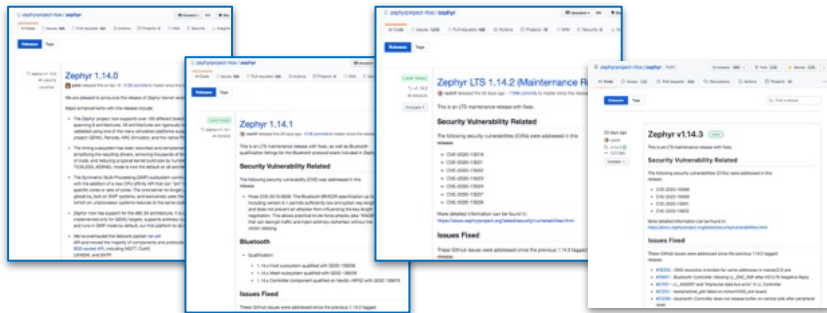
github.com/zephyrproject-rtos/zephyr/releases/tag/zephyr-v3.7.0

Long Term Support (LTS 1 & LTS 2)



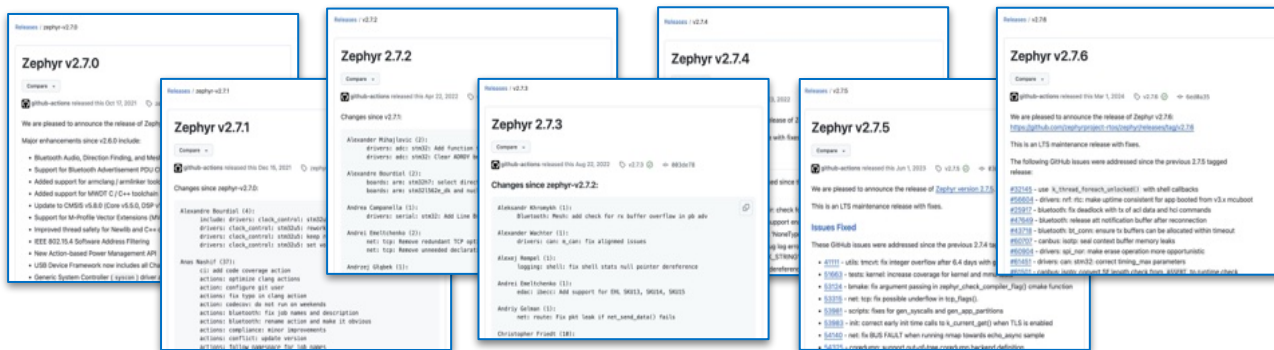
LTS 1

Apr '19 → Nov '21



LTS 2

Oct '21 → Mar '24



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
```



zephyr.spdx	SBOM for the Zephyr source files actually used by your application
modules.spdx	SBOM for the modules being used
app.spdx	SBOM for the source files of your application
build.spdx	SBOM for all the build objects , inc. of course your final image

SBOMs at Scale...Automatically



708 boards

13 apps

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

A screenshot of the Zephyr Dashboard 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 table of boards. The table has columns for board names and five status columns. The status columns are labeled "11 PASSED", "7 PASSED", "8 PASSED", "11 PASSED", and "6 PASSED". The board names listed include "HELLO WORLD", "PHILOSOPHERS", "SHELL MODULE", "TENSORFLOW LITE MICRO", and "MICROPYTHON". A detailed view of the "Andes ADP-XC7K AE350" board is shown, with status buttons for "PASSED", "GENERATED", "PASSED", and "PASSED". A "Download SBOM" button is visible in the detailed view. The "BUILD DETAILS" section on the left includes "SHOW SIMULATION" and "CONTACT US FOR RENODE SUPPORT SERVICES".

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

CVE Numbering Authority



- [Registered with MITRE](#)
in 2017
 - Zephyr triages and issue our own CVEs
- **Zephyr Project Security Incident Response Team (PSIRT)**
 - Volunteers from the Security Committee
 - Led by the Zephyr Security Architect.

The screenshot shows the Zephyr Project website. At the top, there is a navigation bar with the following links: About, Partner Information, Program Organization, Downloads, and Resources & Support. Below the navigation bar, the page title is "Zephyr Project". A note states: "Links that redirect to external websites will open a new window or tab depending on the web browser used." Below this, there is a section titled "Steps to Report a Vulnerability or Request a CVE ID" with two steps: "Step 1: Read disclosure policy" with a link "View Policy", and "Step 2: Contact" with a link "Email". Below the steps is a table with the following details:

Scope	Zephyr project components, and vulnerabilities that are not in another CNA's scope.
Program Role	CNA
Top-Level Root	MITRE Corporation
Security Advisories	View Advisories
Organization Type	Vendor Open Source
Country*	USA

* Self-identified by CNA

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 heading is "Product Creators Vulnerability Alert Registry". Below the heading, there is a section for "Criteria for Participation" with three bullet points: "Have a product that will respond to public public advisories and professionals how Zephyr is being used in the product.", "Have a publicly shared product based on core values of Zephyr", and "Have an already documented security program.", followed by a note that the Zephyr Embargo Policy must be satisfied. A "Removal" section states that if a member stops adhering to these criteria after joining the list, their membership will be unenforced. A link is provided for "More information on Zephyr's Security and Disclosure practices can be found at Security". The form contains several input fields: "First name*", "Last name*", "Email*", "Phone number", "Company name*", "Job title*", "Link to your Company's Product that is built with Zephyr SDKs, e.g. https://www.zephyrproject.org/", and "Zephyr release in use?". A "Zephyr Embargo Policy" section explains that information is shared with other members of the team and is subject to the team's explicit approval. It also states that members must agree to the embargo policy and that the information will be kept confidential. At the bottom, there is a checkbox for "I agree to receive other communications from The Linux Foundation." and a "Submit" button.

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.

FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33 | EXECUTIVE SUMMARY

AMNESIA:33

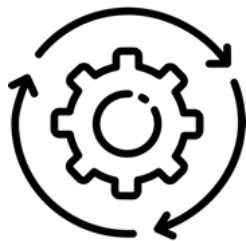
Research Report Executive Summary

150+ VENDORS AFFECTED

- Forescout 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.

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

Zephyr Security Summary



Weekly Coverity scans

MISRA scans

Automated Code checks
per pull request



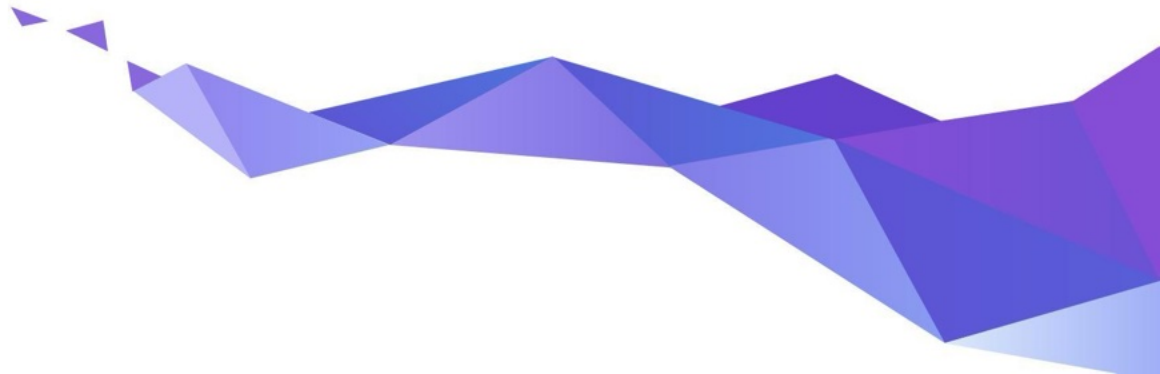
[Documented secure coding practices](#)

Vulnerability response
criteria publicly
documented



SBOM generation per
[ISO/IEC 5962:2021](#)

Certification



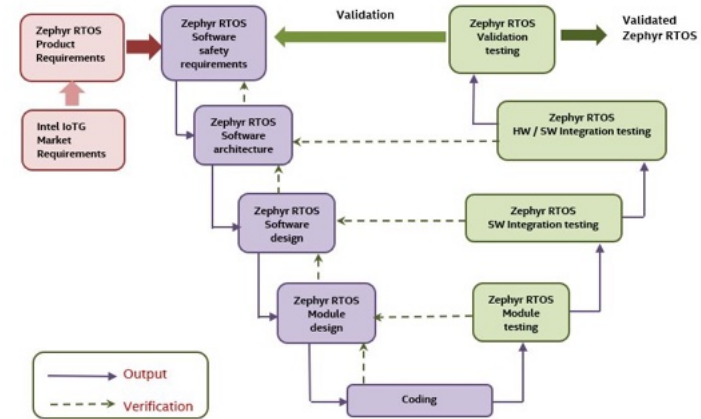
Compliant Development: V-model



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

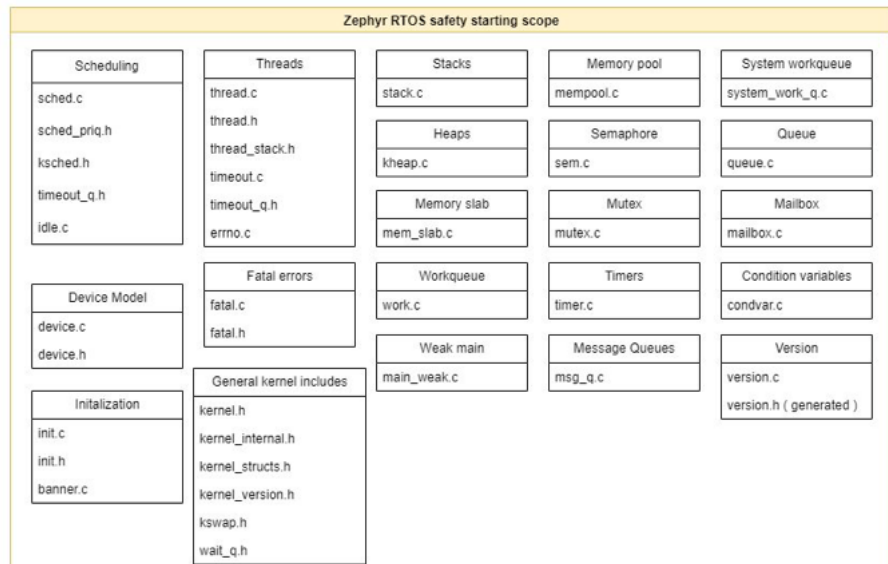


Draft (Pending Approval by Certification Authority)			
Artifacts	Type of Doc	Owner	Work in progress Visibility
Plans	Category		
Safety Development Plan	Plan/Process	Safety Committee	Public - Project Docs
Safety Assessment Plan	Plan/Process	FSM	Safety Committee Github
Verification / Validation / Integration 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
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
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			
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.

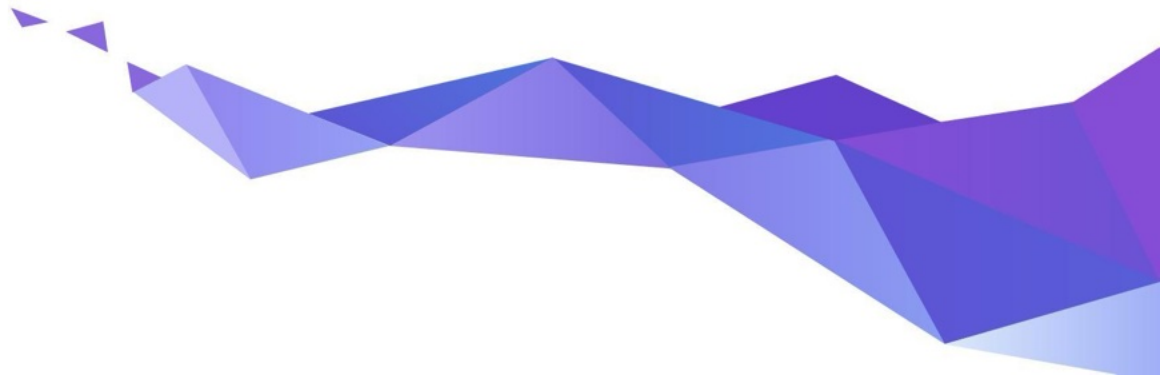
Initial certification focus

- 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



7/LAB

ǝC6

ALIF
SEMICONDUCTOR

ARDUINO

arm

Baumer
Passion for Sensors

Baylibre

BENINGO
EMBEDDED GROUP

Blecon

blues wireless

Canonical

JRJC
菁蓉联创

DOULOS

embedd|

Embeint

ezurio

HONDA
The Power of Dreams

hubble
NETWORK

iar

infineon

inovex

linaro

MICROCHIP

oticon
life-changing technology

perceptio

Qt Group

RAYTAC

REALTEK

Savoir-faire
LINUX

Schneider
Electric

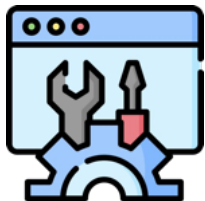
ST

SYNOPSIS

tenstorrent

TEXAS
INSTRUMENTS

Vibrant Ecosystem



Development Tools



Governing Board

Technical Steering Committee

Contributors



Applications & Middlewares



Training & Consulting



Firmwares & Libraries

Ecosystem // Developer Tools



Development Tools



Training & Consulting



Firmwares & Libraries



Applications & Middlewares

IDE



Compilers



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

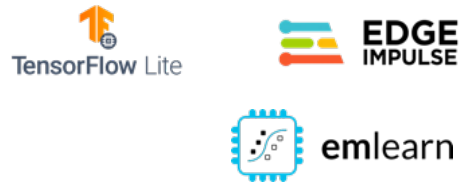


Applications & Middlewares

Security



TinyML



Language runtimes



Others



Ecosystem // Apps & Middlewares



Remote Management



Graphical Interfaces



Robotics



Training & Consulting

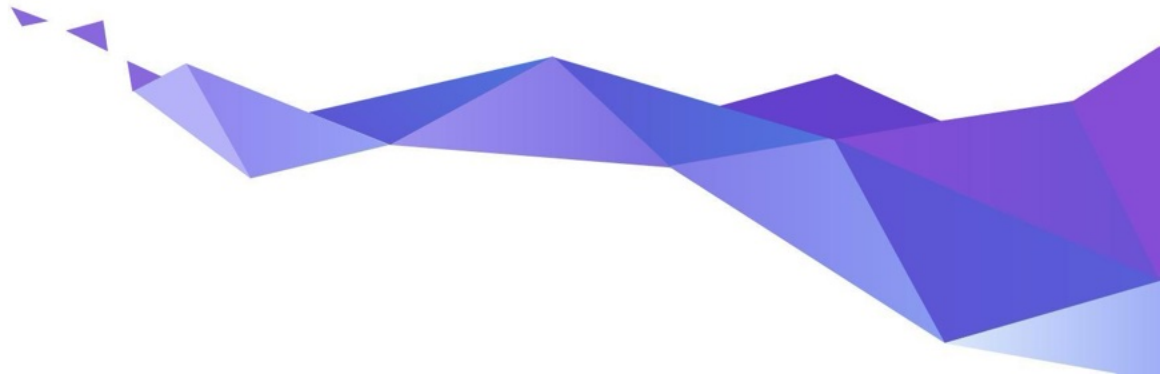


Firmwares & Libraries



Applications & Middlewares

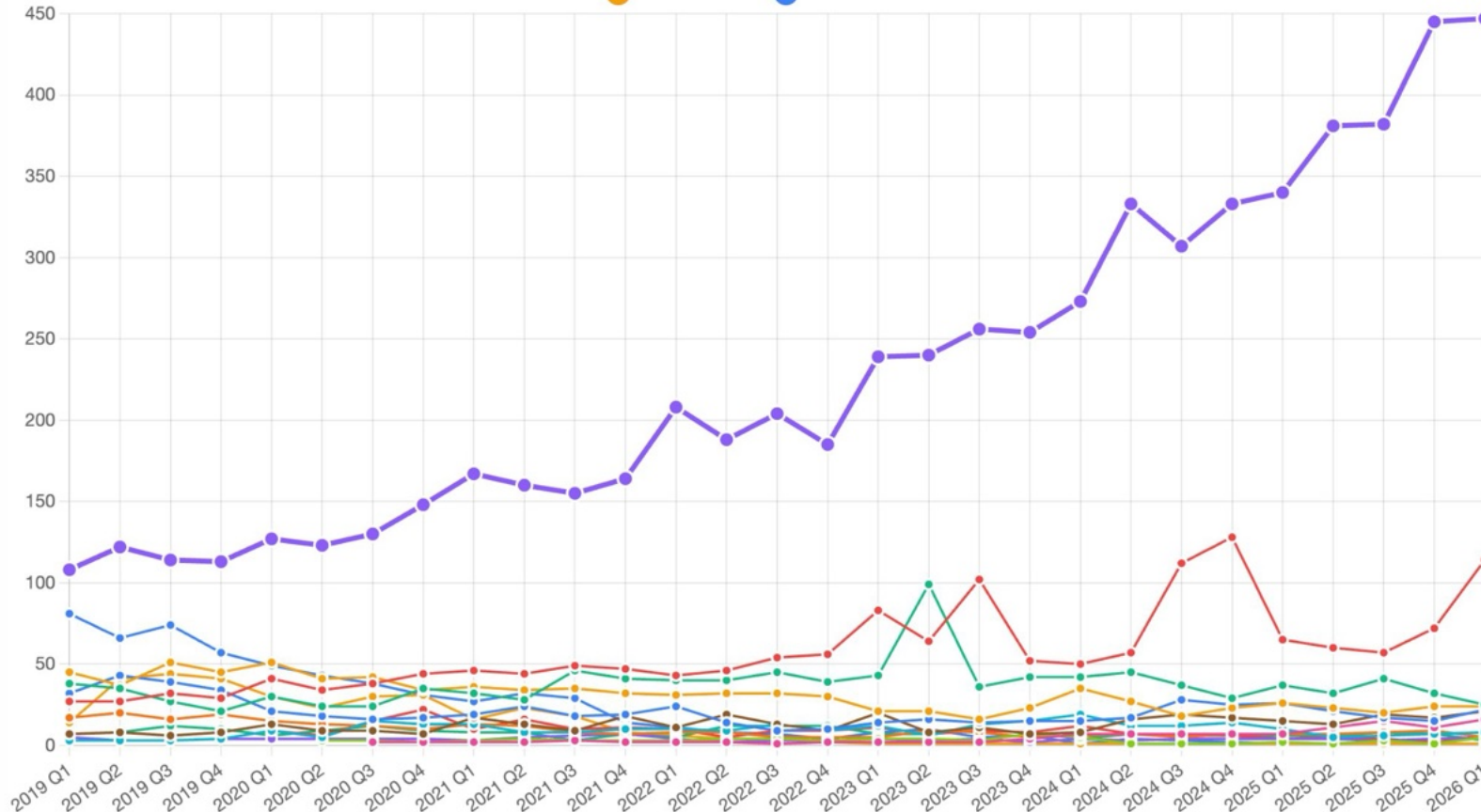
Zephyr in the RTOS landscape



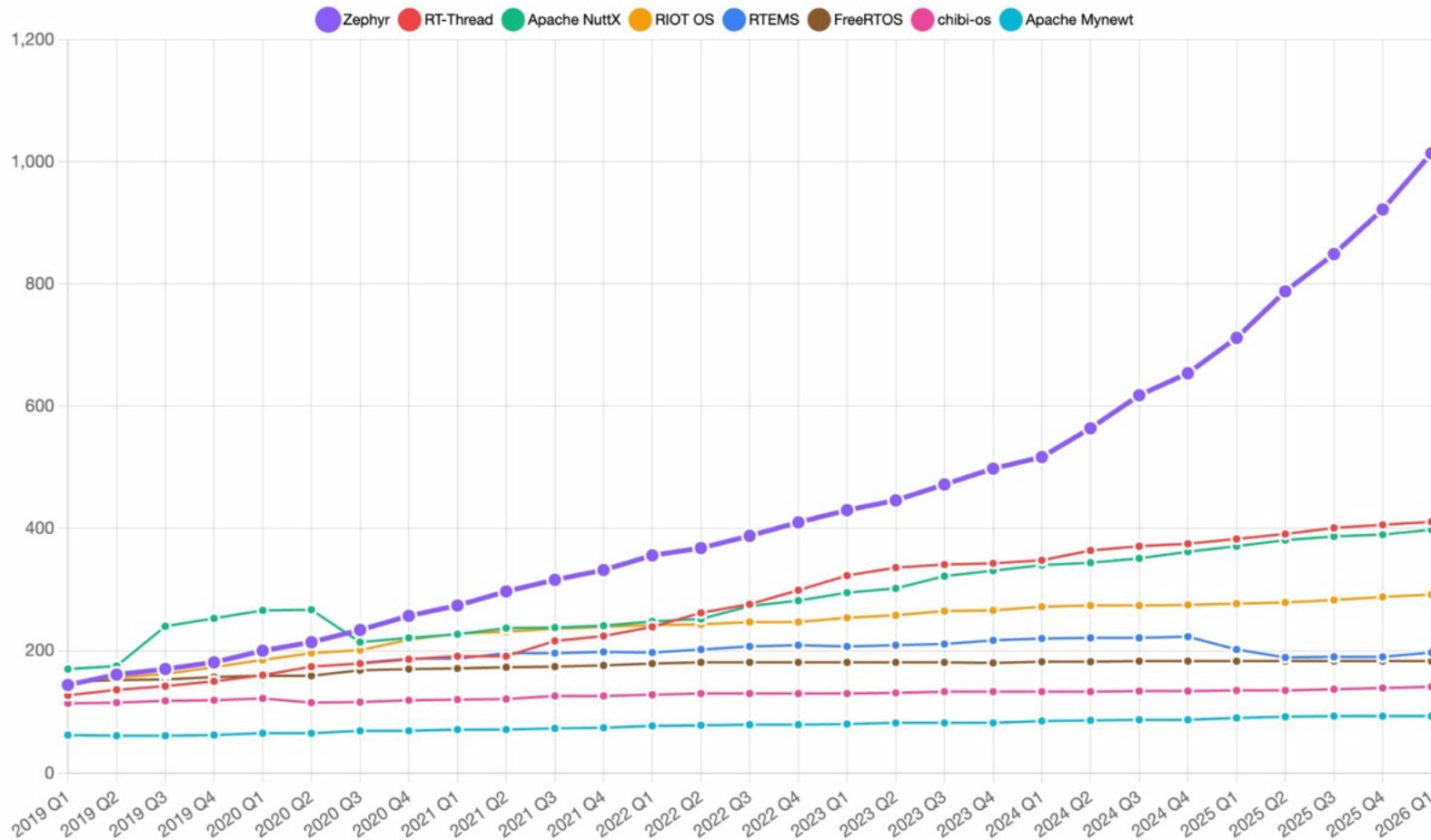
Unique Contributors per Month



- Zephyr
- Apache NuttX
- RT-Thread
- RIOT OS
- TizenRT
- RTEMS
- Ariel OS
- FreeRTOS-Kernel
- Eclipse ThreadX
- Apache Mynewt
- chibi-os
- FreeRTOS
- Contiki-NG
- Amazon FreeRTOS
- Arm Mbed OS

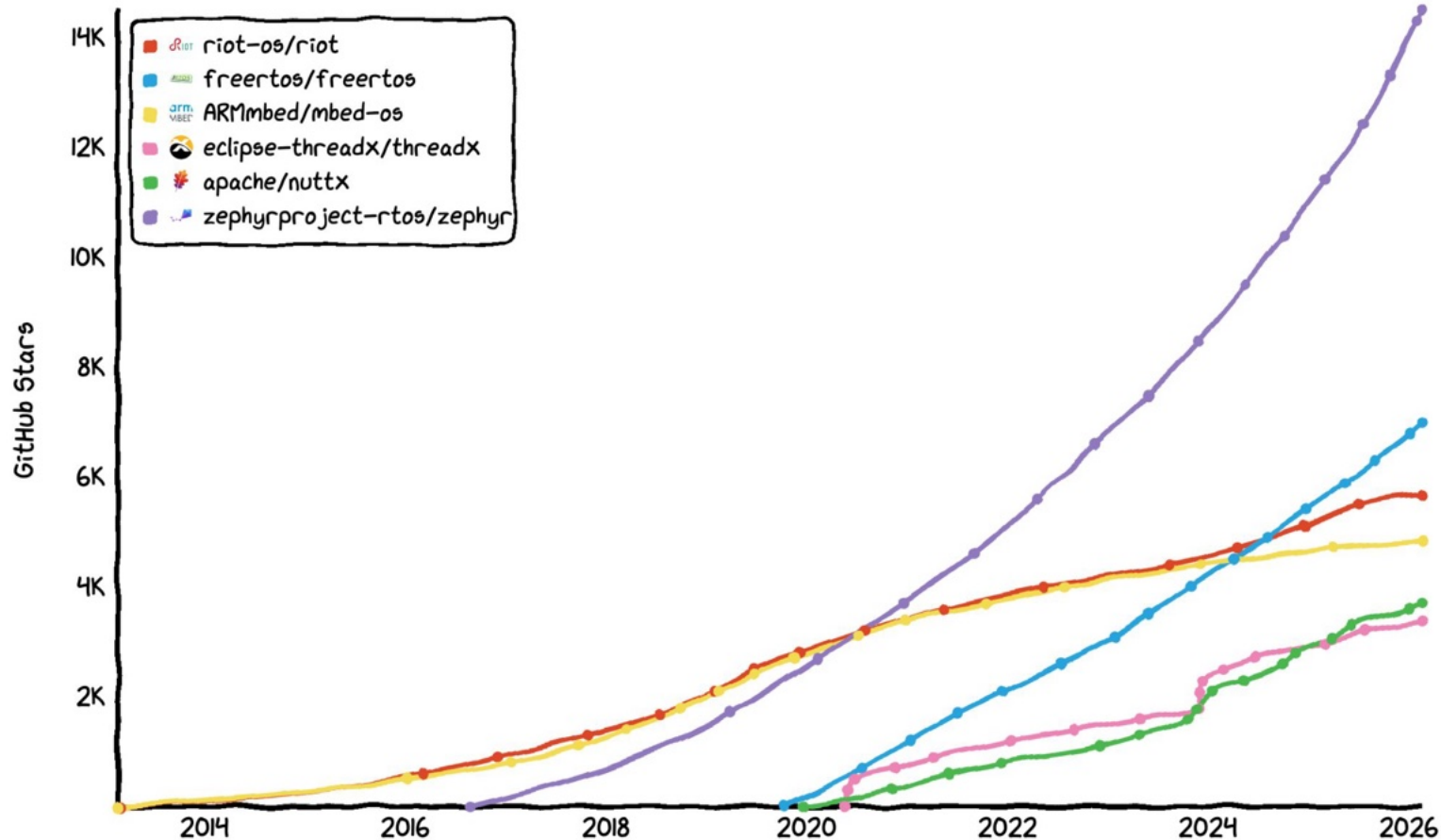


Supported Boards



Note: Only the operating systems for which number of supported boards could be easily computed automatically are included on this chart.

Star History



GitHub Clones & Unique Visitors



242,963 Views

21,460 Unique visitors

2025-04-23 → 2025-05-06

~1183 unique clones per day

~1532 unique visitors per day



143,575 Clones

16,571 Unique cloners

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



github.com/zephyrproject-rtos



lists.zephyrproject.org



chat.zephyrproject.org



zephyrproject.org

