Zephyr Project Overview

A proven RTOS ecosystem, by developers, for developers
Use cases for a real-time OS

- Industrial IoT
- Asset Tracking
- Wearables
- Automotive
- Healthcare
- Worker Safety
SMALL yet SCALABLE

< 8KB Flash
< 5KB RAM

from small sensor nodes... to complex multi-core systems
FLEXIBLE

Heavily customizable
Out-of-the-box support for 450+ 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

- **Comprehensive, lightweight, kernel & supporting services**
  - Fits where Linux is too big

- **Inherently portable & secure**

- **Highly connected**
  - Bluetooth 5.0 & BLE
  - Wi-Fi, Ethernet, CANbus, ...
  - IoT protocols: CoAP, LwM2M, MQTT, OpenThread, ...
  - USB & USB-C

- **Developer-friendly**
  - Logging, tracing, debugging, built-in shell, Windows/Linux/macOS support, ...
Products Running Zephyr Today

- Proglow
- Ruuvi Tag
- PHYTEC Distancer
- Keeb.io BDN9
- Hati-ACE
- Oticon More
- Adhoc Smart Waste
- GNARBOX 2.0 SSD
- Anicare Reindeer Tracker
- Safety Pod
- BLiXT solid state circuit breaker
- Moto Watch 100
- Lildog & Lilcat pet tracker
- Rigado IoT Gateway
- Livestock Tracker
- Laird Connectivity sensors & gateways
- BeST pump monitoring
- Vestas Wind Turbines

zephyrproject.org/products-running-zephyr
450+ 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
120+ Sensors Already Integrated

- adt7420
- adxl345
- adxl362
- adxl372
- ak8975
- ang88xx
- ams_as5600
- ams_iAQcore
- apds9960
- bma280
- bmc150_magn
- bme280
- bme680
- bng160
- bmi160
- bmi270
- bmm150
- bmp388
- bq274xx
- ccs811
- dht
- dps310
- ds18b20
- ens
- esp
- fds
- fx
- fxos8700
- ite_tag_i2c
- ite_vcmp_it8xx
- l1s2dh
- l1s2ds12
- l1s2dw12
- l1s2m
- l1s3
- l1s35
- l1s355
- l1s5
- l1s7
- lps22
- lps22ht
- lps25hb
- lsm303dlhc_magn
- lsm6ds0
- lsm6ds1
- lsm6dsd
- lsm303
- lsm304
- lsm305
- max
- max17262
- max30101
- max31875
- max44009
- max6675
- mchp_tach_xec
- mcp9803
- mcu
- cmp
- mhz
- mpr
- mp
- mp
- mpu6050
- mpu9250
- ms5607
- ms5837
- ms5838
- si7210
- si7520
- si7530
- si7540
- sm3511t
- sm32_temp
- stm32_vbat
- stmemsc
- stts751
- sx9500
- th02
- ti_hd
- ti_hdc
- ti_hdc20xx
- tmp007
- tmp108
- tmp112
- tmp116
- vcn14040
- v15310x
- wsen_hids
- wsen_itds

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

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

- ARC
- ARM Cortex-M, Cortex-R & Cortex-A
- Intel x86 & x86_64
- MIPS
- Nios II Processor
- RISC-V 32 & 64 bit
- SPARC
- Tensilica Xtensa

For more details, visit [docs.zephyrproject.org/latest/hardware/index.html#hardware-support](https://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

© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.
Architecture
Diving into Zephyr’s features
IoT Connectivity Options

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

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

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

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

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

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

Describe & configure the available hardware on the target system

Decouple the application from the hardware

&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 = <0x05f>;
    };

    // ...
};

docs.zephyrproject.org/latest/build/dts
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

docs.zephyrproject.org/latest/guides/portability/posix.html
A real-time OS

Benchmark on Arm Cortex-M4F running at 120 MHz

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thread create</td>
<td>2.5 µs</td>
</tr>
<tr>
<td>Thread start</td>
<td>3.6 µs</td>
</tr>
<tr>
<td>Thread suspend</td>
<td>3.3 µs</td>
</tr>
<tr>
<td>Thread resume</td>
<td>3.8 µs</td>
</tr>
<tr>
<td>Context switch (yield)</td>
<td>2.2 µs</td>
</tr>
<tr>
<td>Get semaphore</td>
<td>0.6 µs</td>
</tr>
<tr>
<td>Put semaphore</td>
<td>1.1 µs</td>
</tr>
</tbody>
</table>

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

### Data passing objects available in Zephyr kernel

<table>
<thead>
<tr>
<th>Object</th>
<th>Bidirectional?</th>
<th>Data structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIFO</td>
<td>×</td>
<td>Queue</td>
</tr>
<tr>
<td>LIFO</td>
<td>×</td>
<td>Queue</td>
</tr>
<tr>
<td>Stack</td>
<td>×</td>
<td>Array</td>
</tr>
<tr>
<td>Message queue</td>
<td>×</td>
<td>Ring buffer</td>
</tr>
<tr>
<td>Mailbox</td>
<td>✔</td>
<td>Queue</td>
</tr>
<tr>
<td>Pipe</td>
<td>×</td>
<td>Ring buffer</td>
</tr>
</tbody>
</table>

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.)
Zephyr 3.4 (June 2023) – What’s new?

● New peripherals

Auxiliary displays
NVMe disks & controllers
Retained memory
SMBus
Real-time clocks (RTC)

● Twister improvements (pyTest, Robot Framework, gTest)

● Barrier API

● Snippets ... and more, see Release notes 3.4.
Safety & Security
Code Repositories

Community Contributions via DCO → Development

Forward ports & Keeping Configurations in Sync → Long Term Support “Stable”

Safety & Security Processes → Auditable

Release → LTS Releases

Certifiable Releases
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]
Long Term Support (LTS - 1.14)

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
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

```plaintext
[...]
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
[...]
```
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.
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
Vulnerability Alert Registry

- For an **embargo** to be effective, product makers need to be **notified early** so they can **remediate**
- **Goal**: Zephyr to **fix issues within 30 days** to give vendors 60 days before publication of vulnerability
- Product makers can register to receive these alerts for free by signing up at Vulnerability Alert Registry
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](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17468), and [CVE-2020-17469](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17469), are in the IPv6 Fnet code, one, [CVE-2020-17467](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17467), affects Link-local Multicast Name Resolution (LLMNR), and 2, [CVE-2020-24383](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24383), and [CVE-2020-17470](https://cve.mitre.org/cgi-bin/cvename.cgi?name=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.
Zephyr Security Summary

- Documented secure coding practices
- Vulnerability response criteria publicly documented
- Weekly Coverity scans
  - MISRA scans
- SBOM generation
Certification
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)
- x86 and ARM is initial focus
- Scope will be extended to include additional components as determined by the safety committee
Safety Collateral Proposal

### Draft (pending approval by Certification Authority)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Assumed Collateral</th>
<th>Type of Doc</th>
<th>Owner</th>
<th>Sharing Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Concept</td>
<td>Safety Plan and Safety Assessment Plan</td>
<td>Plan/Process</td>
<td>FSM</td>
<td>Platinum</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Verification / Validation / Integration Test Plans</td>
<td>Plan/Process</td>
<td>Testing WG</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Software Development Plan</td>
<td>Plan/Process</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Configuration and Change Management Plans</td>
<td>Plan/Process</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Software Architecture and Module Design Specification</td>
<td>Plan/Process</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Coding Guideline</td>
<td>Plan/Process</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Tools Documentation</td>
<td>Plan/Process</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Safety Concept</td>
<td>Software Requirements</td>
<td>Code</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Test Phase</td>
<td>Software Safety Requirements Specification</td>
<td>Result Artifact</td>
<td>Safety WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Tests (Integration, Arch / Module, Validation)</td>
<td>Code</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Code Review Report</td>
<td>Result Artifact</td>
<td>Safety WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Verification / Validation / Integration Test Reports</td>
<td>Result Artifact</td>
<td>Testing WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Fault Injection Test Report</td>
<td>Result Artifact</td>
<td>Testing WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Tools Classification</td>
<td>Result Artifact</td>
<td>Safety WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Tools Validation</td>
<td>Result Artifact</td>
<td>Safety WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Traceability Report</td>
<td>Result Artifact</td>
<td>Testing WG/FSM</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Test Coverage Report</td>
<td>Result Artifact</td>
<td>Testing WG/FSM</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Coding Guideline Compliance Report</td>
<td>Result Artifact</td>
<td>Safety WG</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Safety Analysis (e.g., FMEA)</td>
<td>Result Artifact</td>
<td>FSM</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Source Code</td>
<td>Code</td>
<td>TSC</td>
<td>Public</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Software User Manual</td>
<td>Result Artifact</td>
<td>TSC</td>
<td>Platinum</td>
</tr>
<tr>
<td>Detailed Test Phase</td>
<td>Safety Manual</td>
<td>Result Artifact</td>
<td>FSM</td>
<td>Platinum</td>
</tr>
</tbody>
</table>

Silver members have limited access, restricted use to Platinum artifacts based on participation.
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

⇒ Provide the evidences that open source developers can map to compliance and meet all requirements
Ecosystem & Governance
Zephyr Project: Platinum Members

- Analog Devices
- antmicro
- Baumer
- Google
- Intel
- Meta
- Nordic Semiconductor
- NXP
- Oticon
- Qualcomm Innovation Center
- T-Mobile
- ZEISS
Zephyr Project: Silver Members
Vibrant Ecosystem

Development Tools

Governing Board

Technical Steering Committee

Contributors

Applications & Middlewares

Training & Consulting

Firmwares & Libraries

Zephyr®

© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.
Zephyr in the RTOS landscape
GitHub Clones & Unique Visitors

2023-05-06 → 2023-05-19

~476 unique clones per day
~1084 unique visitors per day
Zephyr Participation Information

- zephyrproject.org
- github.com/zephyrproject-rtos
- lists.zephyrproject.org
- chat.zephyrproject.org