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

- **Open source** real time operating system
- **Vibrant Community** participation
- Built with **safety and security** in mind
- **Cross-architecture** with broad SoC and development board support.
- **Vendor Neutral** governance
- **Permissively** licensed - Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**
- **Product** development ready using LTS includes security updates
- **Certification** ready with Auditable
Board Support – 350+ and growing

Arduino Due
Nucleo 103RB
Adafruit Feather
Nucleo64 L476RG
Nucleo F411RE
NRF91 pca10090
Nucleo F334R8
Synopsys EMSK
Minnowboard
Altera MAX10
Nucleo 401RE
Vega Board
ARM V2M MPS2
STM3210c
Atmel SAM E70
NRF51
NXP FRDM K64F
NRF52
Seed Carbon
TI Launchpad Wifi
BBC Microbit
STM32373c
Redbear BLE Nano
96b Neon Key
STM32 Olimexino
STM Mini A15
Seeed Nitrogen
ARM V2M Beetle
Zedboard Pulpino
NXP FRDM-KW41Z
SiFive HiFive1
NXP i.MX RT1050

http://docs.zephyrproject.org/boards/boards.html
## Example of Products Running Zephyr Today

<table>
<thead>
<tr>
<th>Proglove</th>
<th>Rigado IoT Gateway</th>
<th>Adero Tracking Devices</th>
<th>Distancer</th>
<th>Hati-ACE</th>
<th>Oticon More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intellinium Safety Shoes</td>
<td>GNARBOX 2.0 SSD</td>
<td>HereO Core Box</td>
<td>Safety Pod</td>
<td>OB-4</td>
<td>Vestas Wind Turbine</td>
</tr>
<tr>
<td>Point Home Alarm</td>
<td>RUUVI Node</td>
<td>Anicare Reindeer Tracker</td>
<td>Sentrius</td>
<td>See.Sense AIR</td>
<td>Enpointe Relay Box</td>
</tr>
</tbody>
</table>
Zephyr Supported Hardware Architectures

- ARC
- ARM
- Intel
- MIPS
- Nios II
- RISC-V
- Xtensa
Native Execution on a POSIX-compliant OS

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

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

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

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

[Diagram of Zephyr architecture]

POSIX support in Zephyr

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

Fully featured OS allows developers to focus on the application
# Zephyr Development Momentum

<table>
<thead>
<tr>
<th>Metric</th>
<th>LTS 1 (v1.14.0) 2019-4-16</th>
<th>LTS 2 (v2.7.0) 2021-10-18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contributors</td>
<td>500</td>
<td>1000</td>
</tr>
<tr>
<td>Boards</td>
<td>160</td>
<td>350</td>
</tr>
<tr>
<td>Architectures</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Commit Velocity</td>
<td>1.4 [commits / hr]</td>
<td>2.5 [commits / hr]</td>
</tr>
</tbody>
</table>

Results courtesy of Chris Friedt (LTS 2 Release Manager)

Posted: [https://www.zephyrproject.org/zephyr-lts-v2-preview/](https://www.zephyrproject.org/zephyr-lts-v2-preview/)
**Zephyr Social Momentum**

<table>
<thead>
<tr>
<th>Metric</th>
<th>LTS 1 (v1.14.0) 2019-4-16</th>
<th>LTS 2 (v2.7.0) 2021-8-31?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter (followers)</td>
<td>2,378</td>
<td>6,014 (153% 🚀)</td>
</tr>
<tr>
<td>Facebook (followers)</td>
<td>495</td>
<td>706 (42% 🚀)</td>
</tr>
<tr>
<td>LinkedIn (connections)</td>
<td>1,200 (Q3 2020)</td>
<td>3,174 (🚀)</td>
</tr>
<tr>
<td>WeChat</td>
<td>290 (Q4 2019)</td>
<td>380 (🚀)</td>
</tr>
</tbody>
</table>

Results courtesy of Maemalynn Meanor
Just after LTS 1 Github Traffic - 2019/5/7

- Unique clones: 201
- Total clones: 1,118
- Unique visitors: 639
- Total visits: 6,743

LTS 2 pre-release Github Traffic - 2021/10/12

- Unique clones: 533
- Total clones: 3,439
- Unique visitors: 1,966
- Total visits: 11,298
Code Repositories

Forward ports & Keeping Configurations in Sync

Development

Long Term Support "Stable"

Auditable

Community Contributions via DCO

Releases

LTS Releases

Safety & Security Processes

Certifiable Releases
Zephyr OS: Long Term Support (LTS 2.7)

LTS #2 released on 2021/10/16 - it is:

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

It is not:

- A Feature-Based Release: focus on hardening functionality of existing features, versus introducing new ones.
- Cutting Edge
Delivered bug fixes and latest security updates for last 2 years!
Zephyr OS: Auditable

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

- Code bases will be kept in sync.
- More rigorous processes (necessary for certification) will be applied to the auditable code base.

Processes to achieve selected certification to be:

- Determined by Safety Committee and Security Committee
- Coordinated with Technical Steering Committee
Standards Being Pursued

Coding for Safety, Security, Portability and Reliability in Embedded Systems:
- MISRA C:2012, with Amendment 1, following MISRA C Compliance:2016 guidance
- SEI CERT C and JPL (Jet Propulsion Laboratory California Institute of Technology) used as reference

Functional Safety:
- IEC 61508: 2010 (SIL 3 initially, eventually though like to get to SIL 4)
  - Broadest for robotics and autonomous vehicle engineering companies. Reference for other standards in Robotics domain.

Others under consideration:
- Sampled Certifications derived from IEC 61508: Medical: IEC 62304; Auto: ISO 26262; Railway: EN 50128
- Medical: FDA 510(K), ISO 14971, IEC 60601; Industrial: UL 1998, ??
Building in Safety for LTS → Auditable

  - Representatives from Parasoft, Intel, Synopsys, Google, NXP, Baumer, etc.
  - Work closely with the **TSC**

- Initial target is **IEC 61508 SIL 3 / SC 3** (IEC 61508-3, 7.4.2.12, Route 3s) for a limited scope.

- Multiple safety activities in progress to establish **safety plan, coding guideline compliance, traceability, requirements, test coverage, tooling**, etc.
  - LTS 2 is starting point for Auditable, branch made November 2021
  - Zephyr Project [Coding Guidelines](https://www.zephyrproject.org/docs/Coding-Guidelines) based on MISRAC:2021

- Engagement with **FSM** and **certification authority**.
  - FSM on board June 2021, safety plan drafting in progress
  - Certification Authority engagement targeted Q1 2022
Zephyr OS: Initial Certification Focus

- Start with a limited scope
- x86 and ARM arch
- Scope will be **extended** to include additional components as determined by the safety committee
  - Some of the modules under consideration for the next iteration include: Crypto, IPC, Flash, etc.
Zephyr OS: High-level Certification Roadmap

Pre Q4’21
- Certification Scope Defined
- Safety Plan
- Coding Guidelines Approved
- Test Case Development / Code Coverage
- Safety Manager On Board

Q4’21
- v2.7-auditable-branch Created from LTS2
- Requirements
- Coding Guideline Compliance

Q1’22
- Certification Authority Engagement

Q2’22 →

Safety Documentation for Certification:
- Validation / Verification Test Specs, Reports, Etc.
- Safety Analysis (FMEA; FFI)
- Compliance Matrix
- Traceability Matrix
- Safety Manual
- ETC.

Key:
- Purple: Documentation
- Yellow: Tooling
- Blue: Code
- Green: Other

*Updated Q4’21
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
- Goal is to provide the evidences that open source developers can map to compliance and meet all requirements
System Configurations

- **Single Core MCU**
  - Unicore SoC
  - Core 1

- **Supported with OpenAMP**
  - Zephyr
  - Linux
  - Multicore SoC
  - Core 1
  - Core 2

- **Supported on some architectures**
  - Zephyr
  - Hypervisor
  - SoC
  - Core 1
  - Core 2

- **Supported with ACRN**
  - Zephyr
  - Linux
  - Hypervisor
  - Core 1
  - Core 2

- **Supported with Bluetooth & 15.4**
  - Mesh

Safety and security can apply to all these configurations.
Zephyr Security Summary

- Established Security Committee at project launch in 2016 – meets bi-weekly.
- Secure Coding Practices have been publicly documented for project.
- Zephyr Project registered as a CVE Numbering Authority with MITRE since 2017.
- “Gold” Best Practices Badge criteria Core Infrastructure Initiative met in 2018
- Leveraging Automation to prevent security regressions:
  - Weekly Coverity Scans to detect bad practices in imported code
  - MISRA scans being incorporated, to evolve to conformance and address issues.
- Vulnerability Management in 2020
  - Vulnerability response criteria publicly documented
  - Product makers can register for free for notification of Zephyr
- supporting SBOM generation in 2021
  - Source SBOM’s for releases and updates going forward from version 2.5
  - Ability to automatically generate SBOM for built images included in version 2.6
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
OpenSSF Best Practices Gold Badge

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

- 2020 bulk a vulnerability report highlighted need to document process
- Added vulnerability reporting to project docs

Process:
  - Embargo period
  - Stages issue goes through
  - Working with maintainers to see issues fixed
  - Public disclosure at end
**CVE Numbering Authority with PSIRT**

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

<table>
<thead>
<tr>
<th>Zephyr Project</th>
<th>Zephyr project components, and vulnerabilities that are not in another CNA’s scope</th>
<th><a href="mailto:vulnerabilities@zephyrproject.org">vulnerabilities@zephyrproject.org</a></th>
<th>Zephyr Disclosure Policy</th>
<th>Zephyr Security Advisories</th>
<th>Vendors and Projects</th>
</tr>
</thead>
</table>
Vulnerability Alert Registry

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

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

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

- Secure Coding Practices have been documented for project.
- Zephyr Project registered as a CVE Numbering Authority with MITRE.
- Security Working Group has vulnerability response criteria publicly documented
  - addressed weaknesses and vulnerabilities already
- “Gold” Best Practices for projects as defined by CII
  - https://bestpractices.coreinfrastructure.org/projects/74
- Leveraging Automation to prevent regressions:
  - Weekly Coverity Scans to detect bad practices in imported code
  - MISRA scans being incorporated, to evolve to conformance and address issues.
Advisory Issued by project on 20201208:

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

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

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

- None of the affected code has been used in the Zephyr project, while 1.14 does use the Fnet TCP, it does not use the affected IPv6, DNS or LLMNR code.

https://www.zephyrproject.org/zephyr-security-update-on-amnesia33/
WIP: Improve vulnerability tracking automation

ICS Advisory (ICSA-21-119-04)

Multiple RTOS (Update A)
Original release date: May 06, 2021 | Last revised: May 10, 2021

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

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

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

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

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

- For an **embargo to 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](#).
Robust Ecosystem Supports Zephyr OS

• The Zephyr community provides more than just a high quality, open source operating system
• Applications and middleware providers supplement user-written layers of the software stack
• Developers have choice in robust development and debug tool environments
• Consulting and training providers offer assistance developers may need
Development Tools For Zephyr OS

- **Tracing / Debug Tools**: percepio, SEGGER
- **IDE / Debug Tools**: LAUTERBACH DEVELOPMENT TOOLS, RENODE
- **Debug Tools**: GNU Compilers / Debug Tools
- **Simulation / Testing**: DesignWare ARC

- **Applications & Middleware**: Metaware DT
- **Cloud Debugging**: Platform.io IDE
- **IDE**: Memfault, eclipse

- **SDK**: Goliath, NORDIC SEMICONDUCTOR, SYNOPSYS
- **NXP**: NXP MCUXpresso
Firmware/Middleware/Apps For Zephyr OS

Scientific Library
AI/ML Library
Python
Javascript

Firmware/ IoT monitoring
Intel ZephyrJS Javascript
Firmware
IoT

Application & Middleware
Development Tools

Training & Consulting

Sound Open Firmware
Mbed TLS
Crypto Libraries
SSL/TLS
Zephyr OS Training and Consulting

Services & Consulting
- antmicro
- NXP
- WNDRVR

Services
- AVSystem
- Laird
- Baylibre

Consulting
- The Linux Foundation
- Percepio

Training & Consulting
- Applications & Middleware
- Development Tools
Zephyr & the Edge/Cloud Ecosystem

Carriers
- LTE
- LTE-M
- NB-IoT

Data Analytics & Control
Data Management
Device Management

Edge Gateways/Interfaces
Fog/Mesh

Sensors & Controllers
Smart Devices
(Industrial & Consumer)
Zephyr Project Governance

**Goal:** Separate business decisions from meritocracy, technical decisions

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

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

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

---

**Zephyr Project Governance**

- **Governing Board**
  - Financial & Policy Oversight
  - Marketing Oversight
  - Safety Oversight
  - Security Oversight
  - Kernel & Subsystem Maintainers

- **Technical Steering Committee**
  - Security Architect
  - Safety Architect
  - Architecture Maintainers

- **Contributors**
  - Individual Contributor
  - Member Organizations
  - Supporting Organizations
  - Others

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

Orientation:
• https://www.zephyrproject.org/community/

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

Mail Lists:
• https://lists.zephyrproject.org/g/main

Discord:
• https://chat.zephyrproject.org/ (https://discord.com/invite/Ck7jw53nU2)
Zephyr Project: Platinum Members
Zephyr Project: Silver Members

- Avsystem
- Baylibre
- Foundries.IO
- Goliath
- Infineon
- Laird Connectivity
- Linaro
- Memfault
- Parasoft
- Percepio
- SiFive
- Silicon Labs
- Synopsys
- Texas Instruments
- WNDRVR

and more...