

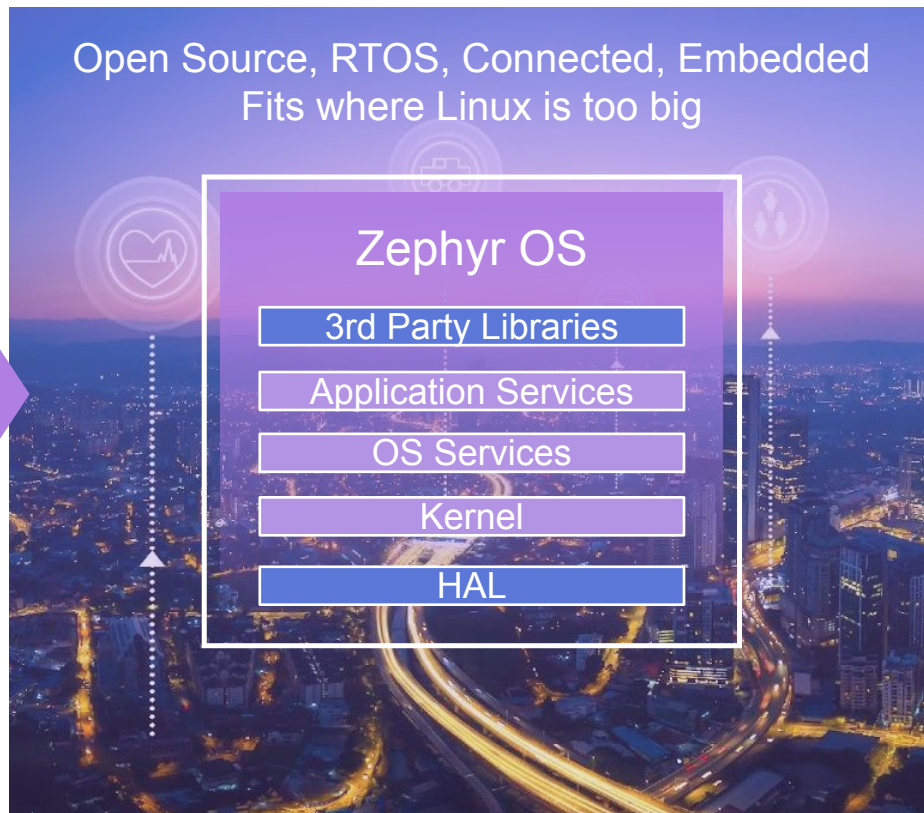
Zephyr Project:

Unlocking Innovation with an
Open Source RTOS

Kate Stewart
@_kate_stewart
kstewart@linuxfoundation.org

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



Products Running Zephyr Today



Grush Gaming
Toothbrush



hereO
Smartwatch



Pro glove



Rigado IoT Gateway



Distancer



Ellcie-Healthy Smart
Connected Eyewear



Intellinium Safety
Shoes



GNARBOX 2.0 SSD



Adero Tracking Devices



Anicare Reindeer
Tracker



Sentrius



GEPS



Point Home Alarm



RUUVI Node



HereO Core Box



Safety Pod

Zephyr Supported Hardware Architectures

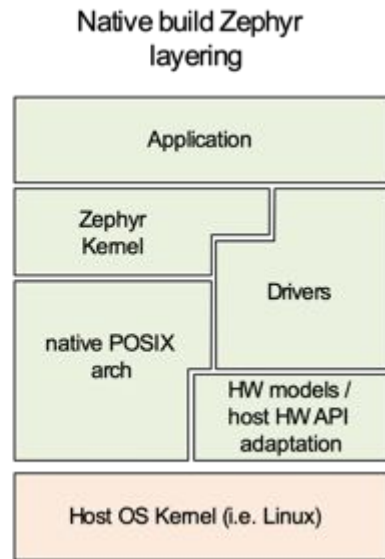
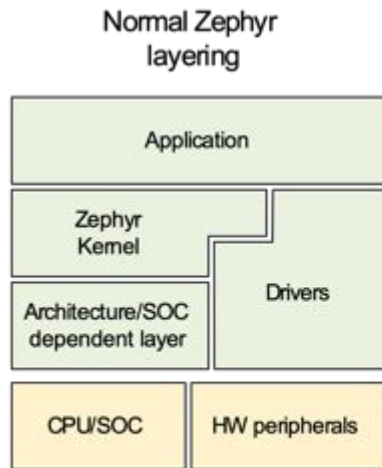


Coming soon:



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

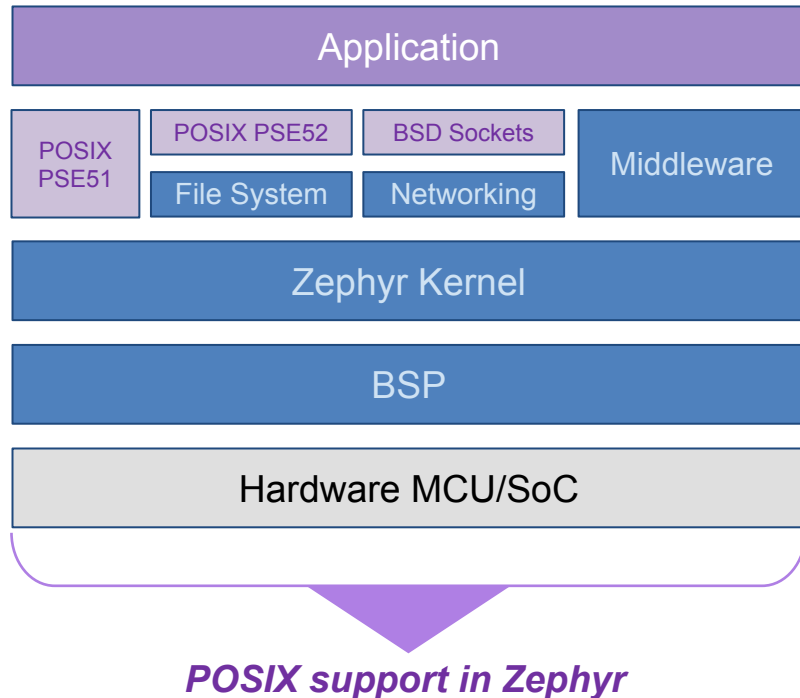


POSIX API on Zephyr

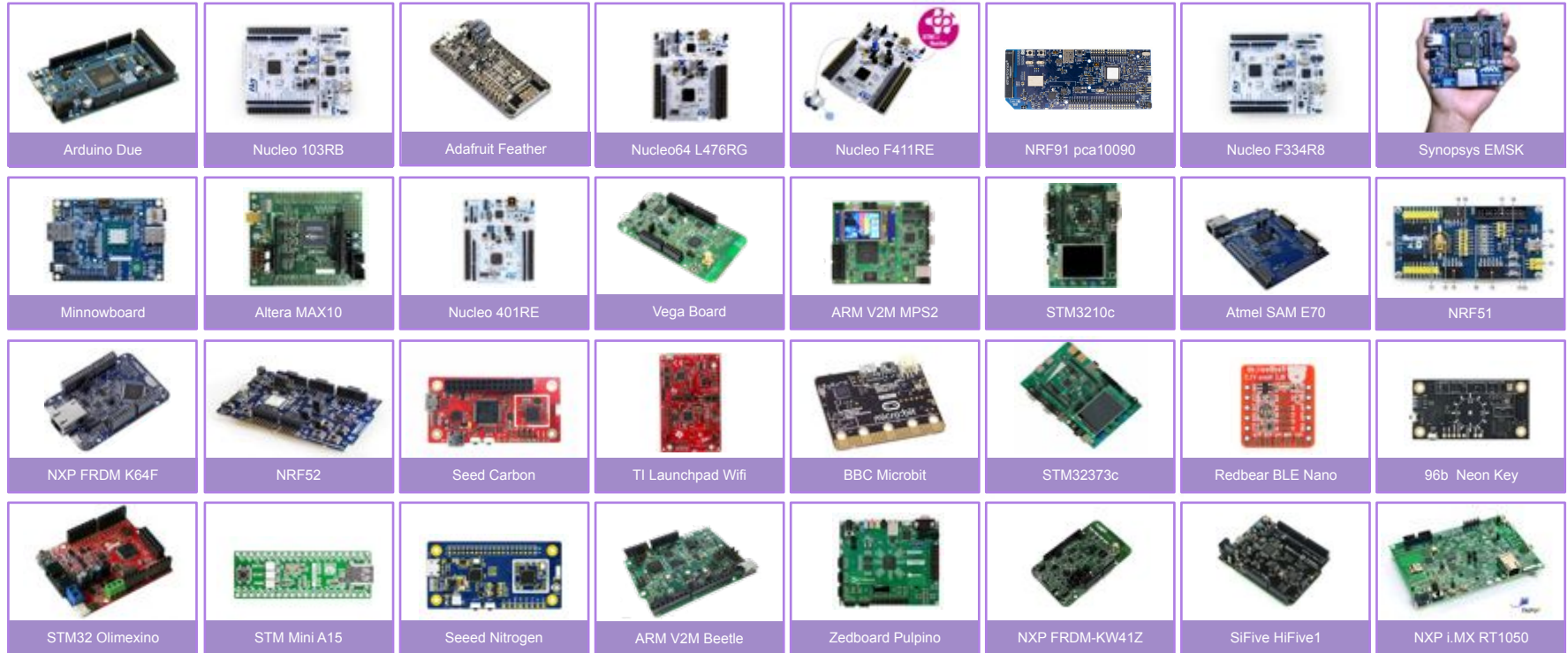
Provides familiar API to non-embedded programmers, especially to Linux developers

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



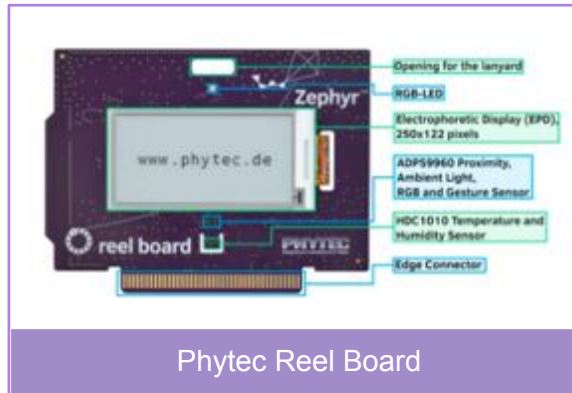
Board Support – 200+ and growing



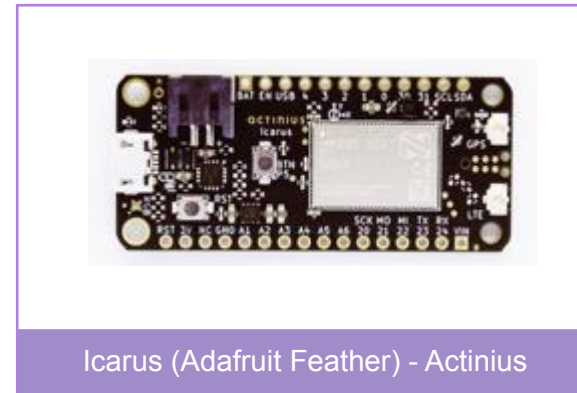
Development Boards Shipping with Zephyr Today



Nordic Thingy91



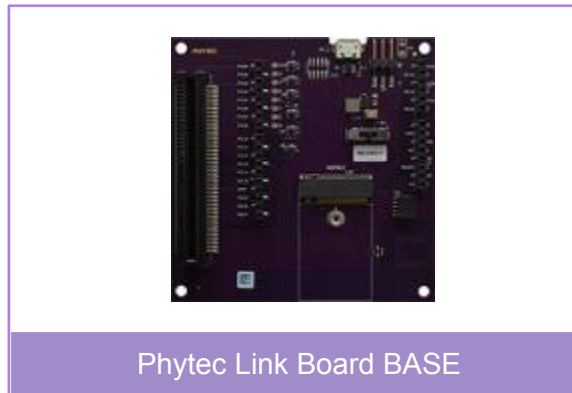
Phytec Reel Board



Icarus (Adafruit Feather) - Actinius



Antmicro Badge

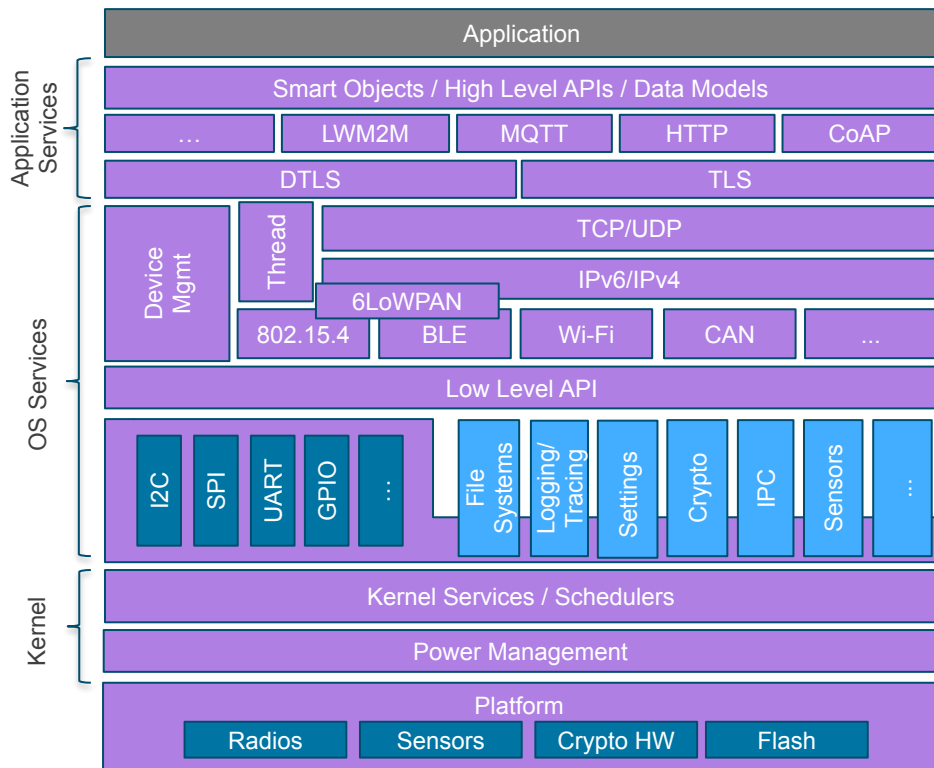


Phytec Link Board BASE



Electronuts Papyr

Architecture

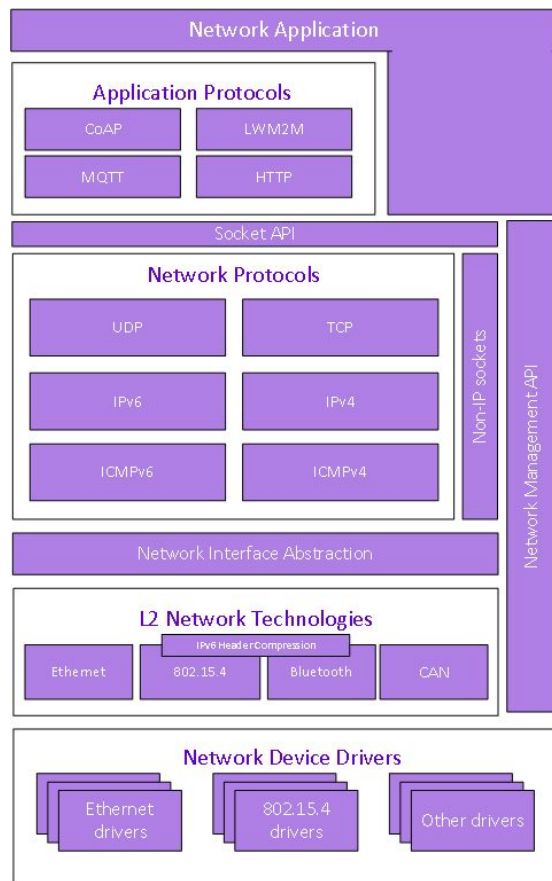


- Highly Configurable, Highly Modular
- Cooperative and Preemptive Threading
- Memory and Resources are typically statically allocated
- Integrated device driver interface
- Memory Protection: Stack overflow protection, Kernel object and device driver permission tracking, Thread isolation
- Bluetooth®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

Fully featured OS allows developers to focus on the application

Native IP Stack

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



Zephyr Networking Features

High-Level Protocols

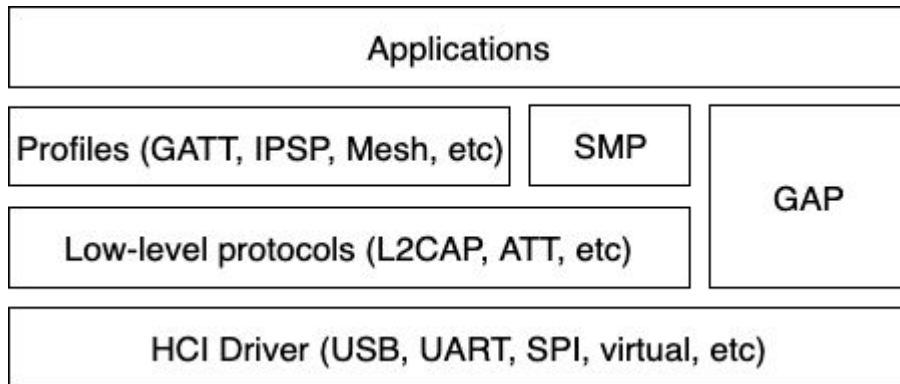
- CoAP v1
- MQTT Client v3.1.1
- HTTP
 - As of Zephyr 2.0 server is implemented using CivetWEB library
 - Native HTTP client
 - Websocket client
- SOCKS5
- LWM2M
- Thread
 - Supported by OpenThread project

Supported technologies

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

Bluetooth Host and Mesh

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



Bluetooth Low Energy Controller

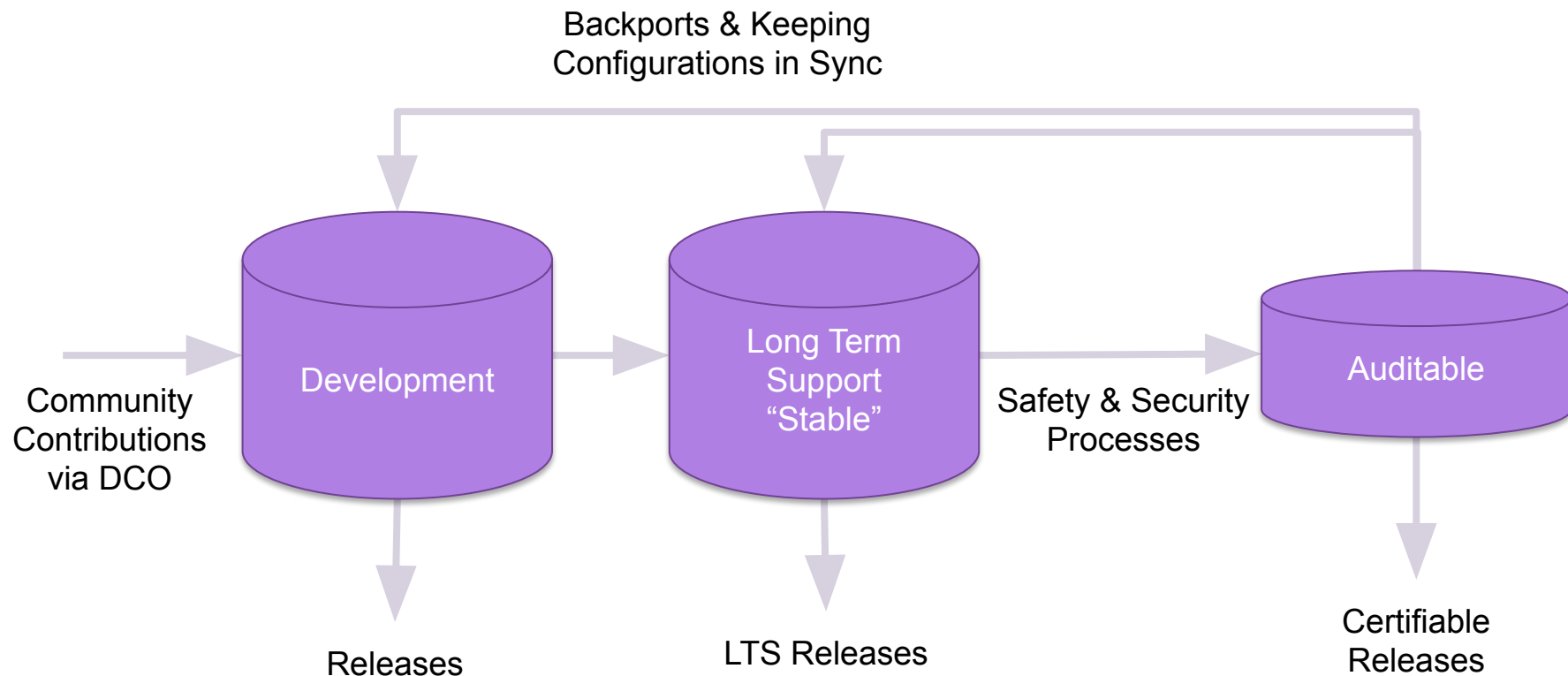
Second-generation open source BLE software Controller:

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

Zephyr USB Device Stack

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

Code Repositories



Zephyr OS: Long Term Support (LTS - 1.14)

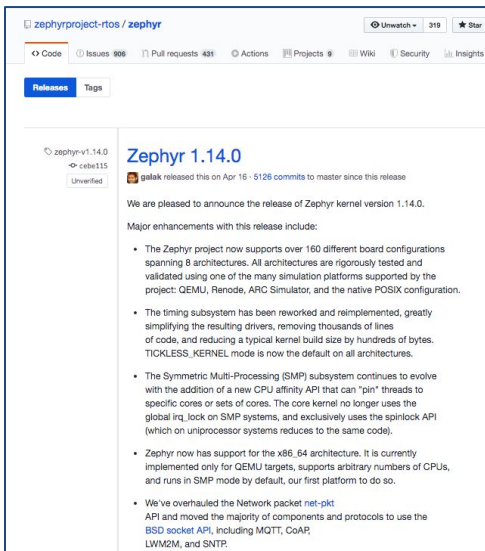
It is:

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

It is not:

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

Zephyr OS: Long Term Support (LTS - 1.14)



zephyrproject-rtos / zephyr

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

Releases Tags

zephyr-v1.14.0
c8e115
Unverified

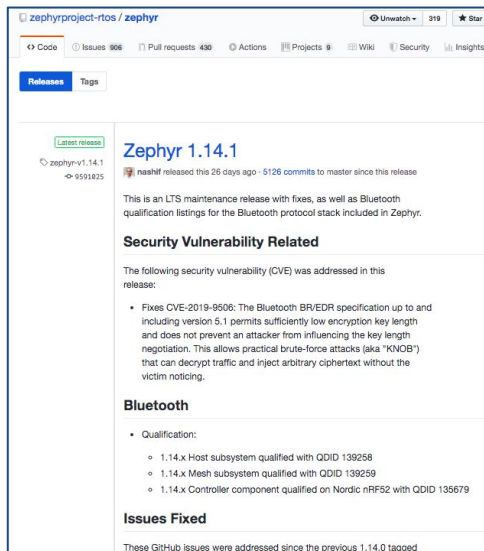
Zephyr 1.14.0

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

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

Major enhancements with this release include:

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



zephyrproject-rtos / zephyr

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

Releases Tags

zephyr-v1.14.1
9591825

Zephyr 1.14.1

nashif released this 26 days ago · 5126 commits to master since this release

This is an LTS maintenance release with fixes, as well as Bluetooth qualification listings for the Bluetooth protocol stack included in Zephyr.

Security Vulnerability Related

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

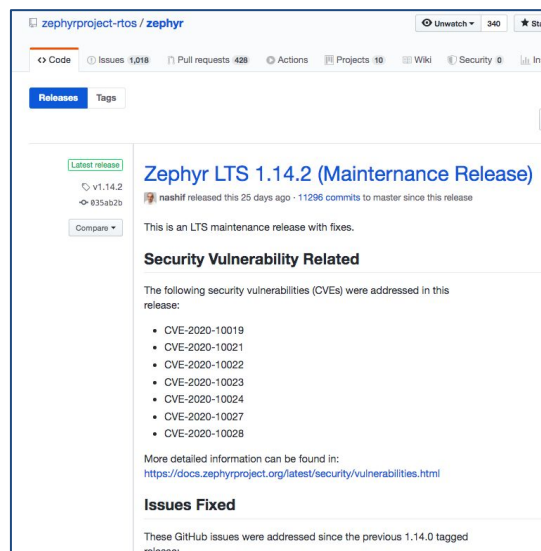
- Fixes CVE-2019-9506: The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject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

Bluetooth

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

Issues Fixed

These GitHub issues were addressed since the previous 1.14.0 tagged



zephyrproject-rtos / zephyr

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

Releases Tags

zephyr-v1.14.2
835a52b
Compare

Zephyr LTS 1.14.2 (Maintenance Release)

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

This is an LTS maintenance release with fixes.

Security Vulnerability Related

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

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

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

Issues Fixed

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

Delivering bug fixes and latest security updates!

Zephyr OS: 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 Under Consideration

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.
 - [Sampled Certifications derived from IEC 61508](#): Medical: IEC 62304; Auto: ISO 26262; Railway: EN 50128

Others:

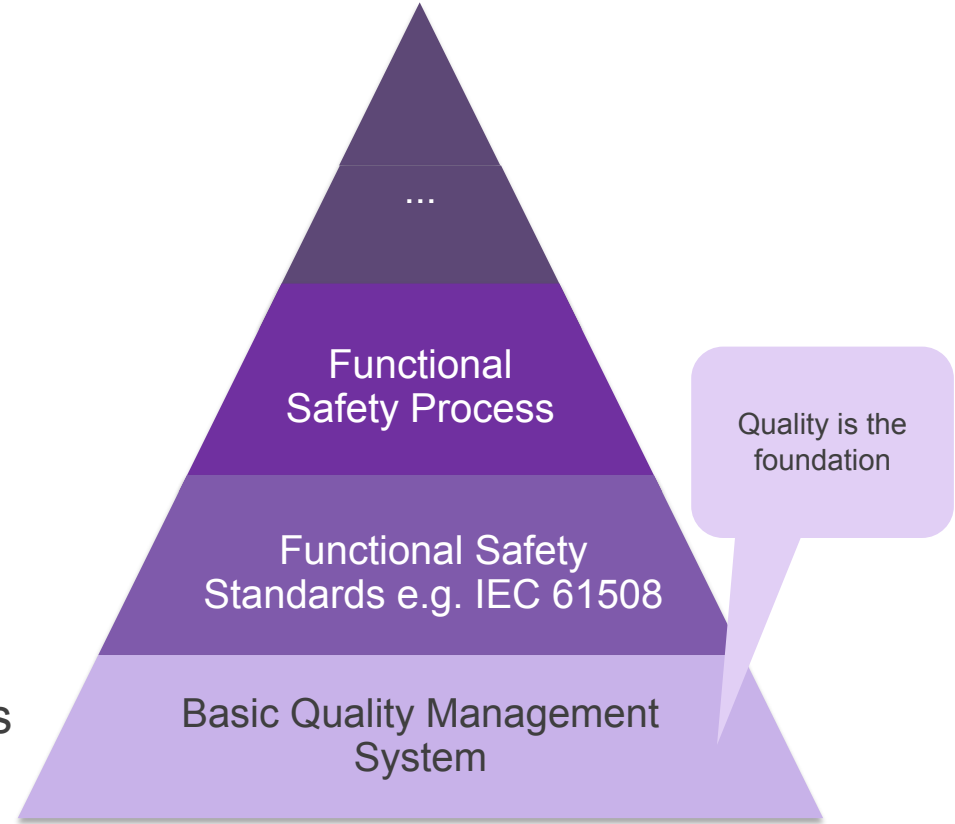
- Medical: FDA 510(K), ISO 14971, IEC 60601; Industrial: UL 1998, ??

Building in Safety for LTS → Auditable

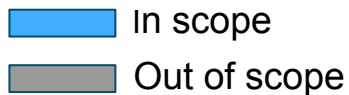
- Established **Safety Committee in 2019**, meets bi-weekly. Community that understands Safety considerations, and implications.
- Initial target was decided by Governing Board to be **IEC 61508** (it is a common basis for others standards that the members care about)
- Build on Coding Practices have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

Zephyr OS: Development

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

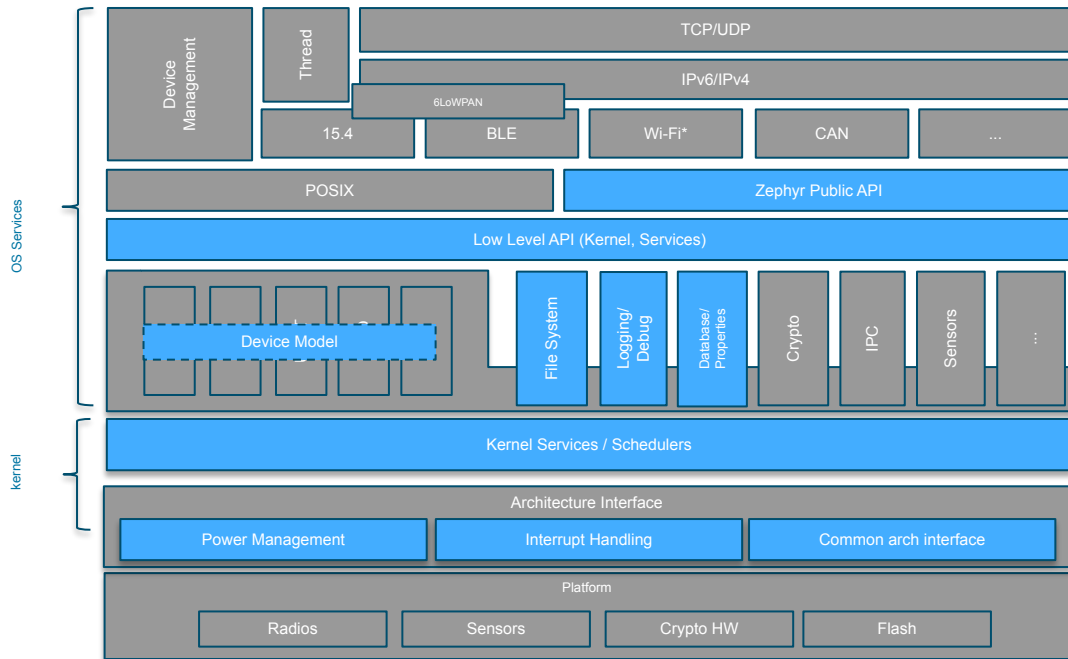


Zephyr OS: Initial Certification Focus

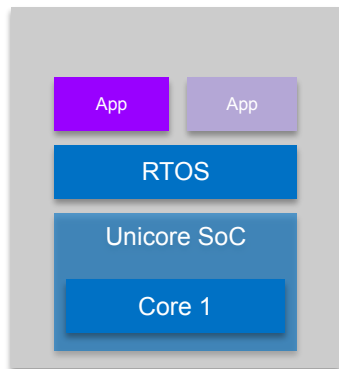


Scope will be **extended** to include **additional components** as determined by the safety committee

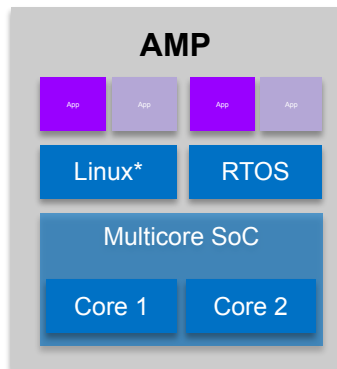
Some of the modules under consideration for the next iteration include: POSIX, Crypto, IPC, Flash, etc.



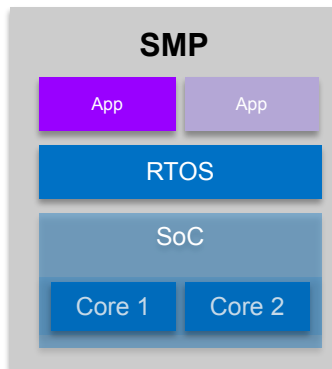
System Configurations



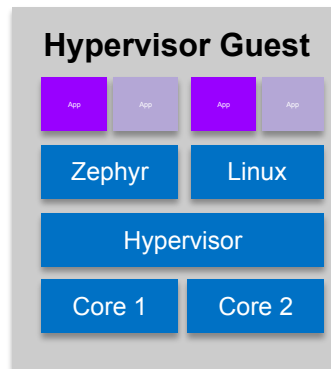
**Single Core
MCU**



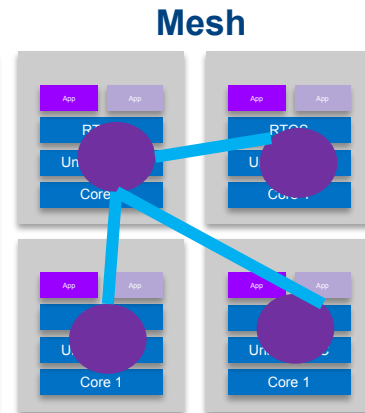
**Supported
with OpenAMP**



**Supported on
some architectures**



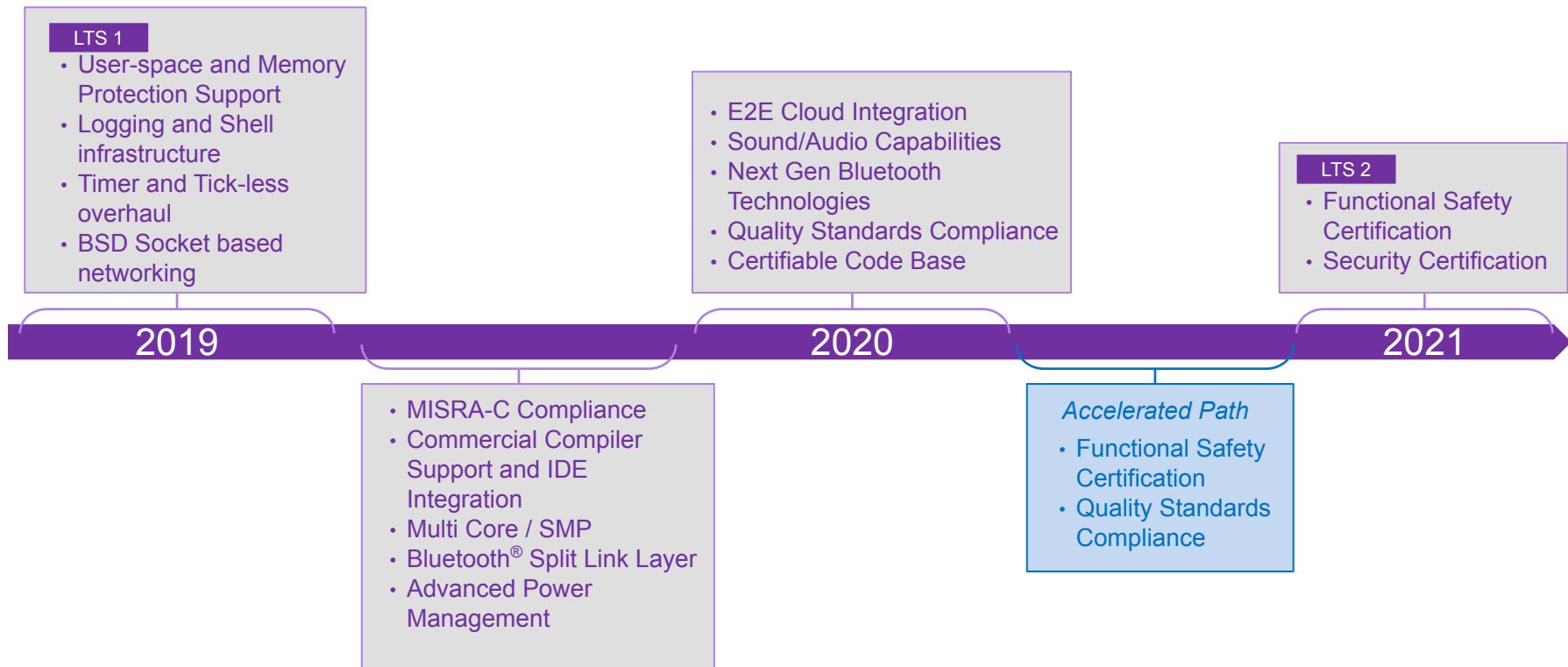
**Supported
with ACRN**



**Supported with
Bluetooth & 15.4**

Safety and security can apply to all these configurations

Zephyr Project Roadmap



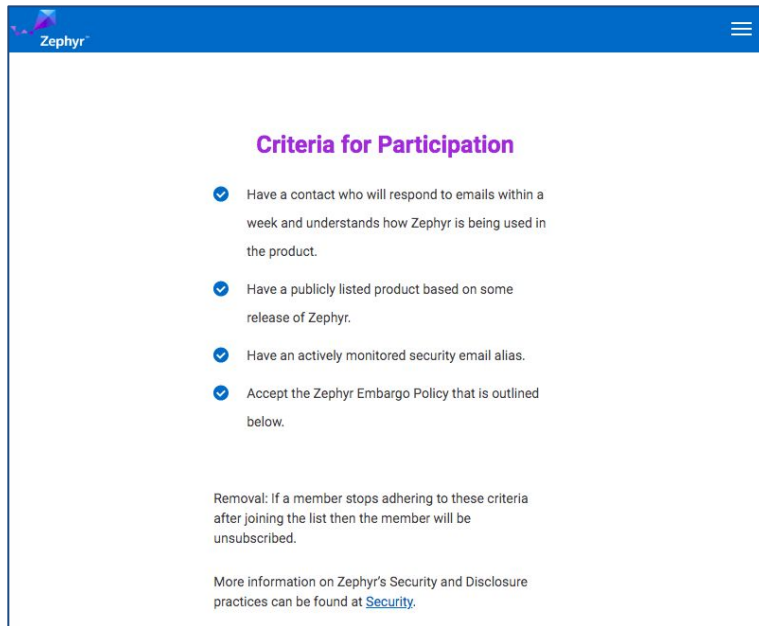
Building in Security for LTS & Auditable

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



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



The screenshot shows the Zephyr website header with the logo and a hamburger menu. The main content area is titled "Criteria for Participation" in purple. It contains a list of four requirements, each preceded by a blue checkmark icon. Below the list, there is a "Removal" section and a link to "Security" for more information.

Criteria for Participation

- ✓ Have a contact who will respond to emails within a week and understands how Zephyr is being used in the product.
- ✓ Have a publicly listed product based on some release of Zephyr.
- ✓ Have an actively monitored security email alias.
- ✓ 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 unsubscribed.

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

Aims: Crypto Drivers

- Same API for different implementations
 - Provided by hardware
 - Atmel ATAES132A
 - Provided by software
 - [TinyCrypt](#) small footprint
 - [mbed TLS](#) feature-rich



Aims: FIPS 140-2/3

- Common for “cryptographic modules”
- Generally, certifies products
- But certification of auditable helps that process
- Focus is on crypto operations



Aims: Secure Boot

Today:

- MCUboot supported by Zephyr
 - Bootloader with revertible upgrades
 - Signed images against public key in ROM
 - Used by TF-M as part of story

Future:

- Upgrade story
- SUIT



Zephyr Ecosystem



Zephyr OS

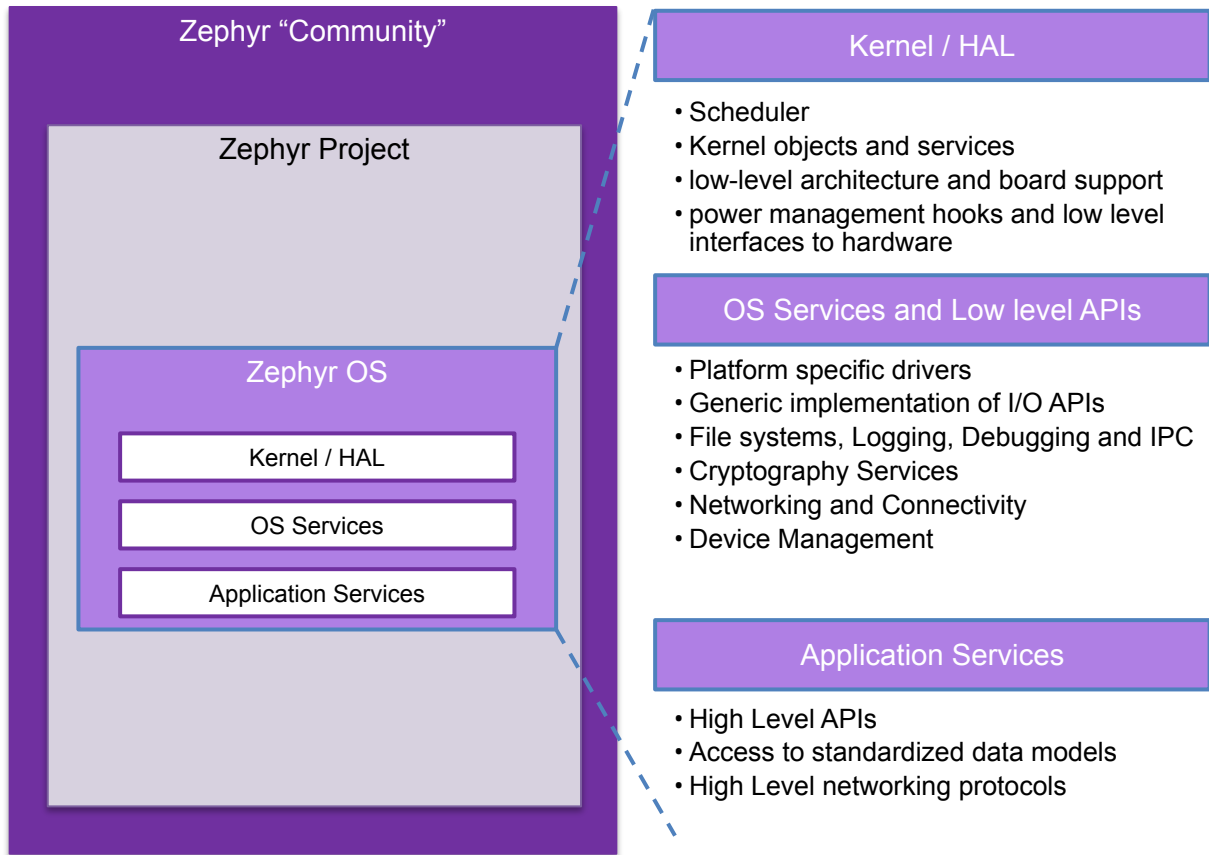
- The kernel and HAL
- OS Services such as IPC, Logging, file systems, crypto

Zephyr Project

- SDK, west, tools and development environment
- Additional middleware and features
- Device Management and Bootloader

Zephyr Community

- 3rd Party modules and libraries
- Support for Zephyr in 3rd party projects, for example: micro-ROS, Tensorflow LITE, Micropython, Jerryscript

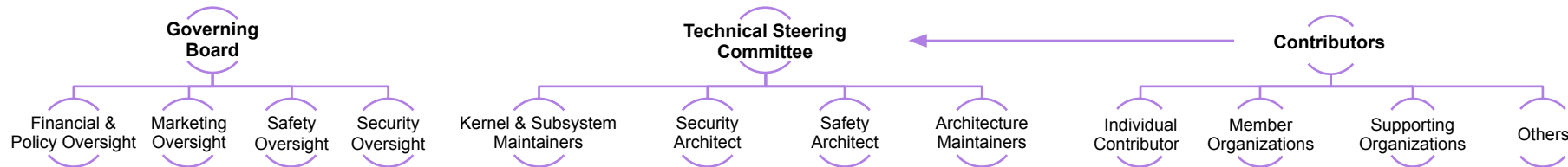


Zephyr Project Members



and more...

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 in RTOS Landscape 2020/07/24

#1

**Total
Contributors**

Rank	RTOS	#
1	Zephyr	726
2	mbed OS	605
3	RT-Thread	284

#1

**Total
Commits**

Rank	RTOS	#
1	Zephyr	42,557
2	nuttX	37,798
3	RIOT	30,552

Upstream Commits in Last Year



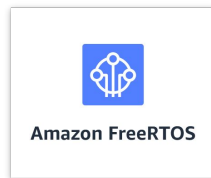
10,000+



5000+



2000+



AliOS | Things

500+



>50



Contiki

Github Web Traffic



2 weeks of traffic to
github.com/zephyr
code repository as
of **2020/06/23**



Growing a Diverse Community!

Lifetime project participation

Authors

• 2016/2: 80
• 2020/7: 726

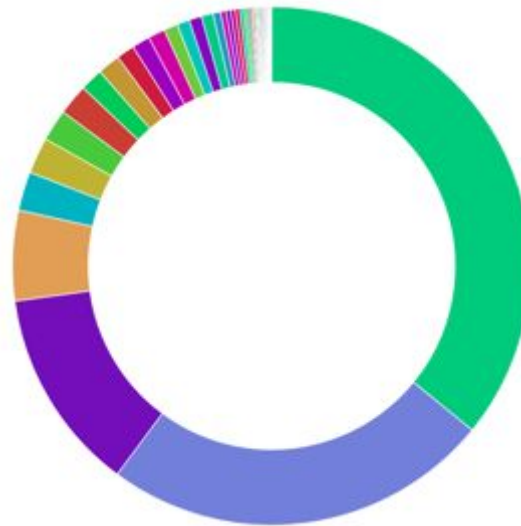
Commits

• 2016/2: 2,806
• 2020/7: 42,557

Boards

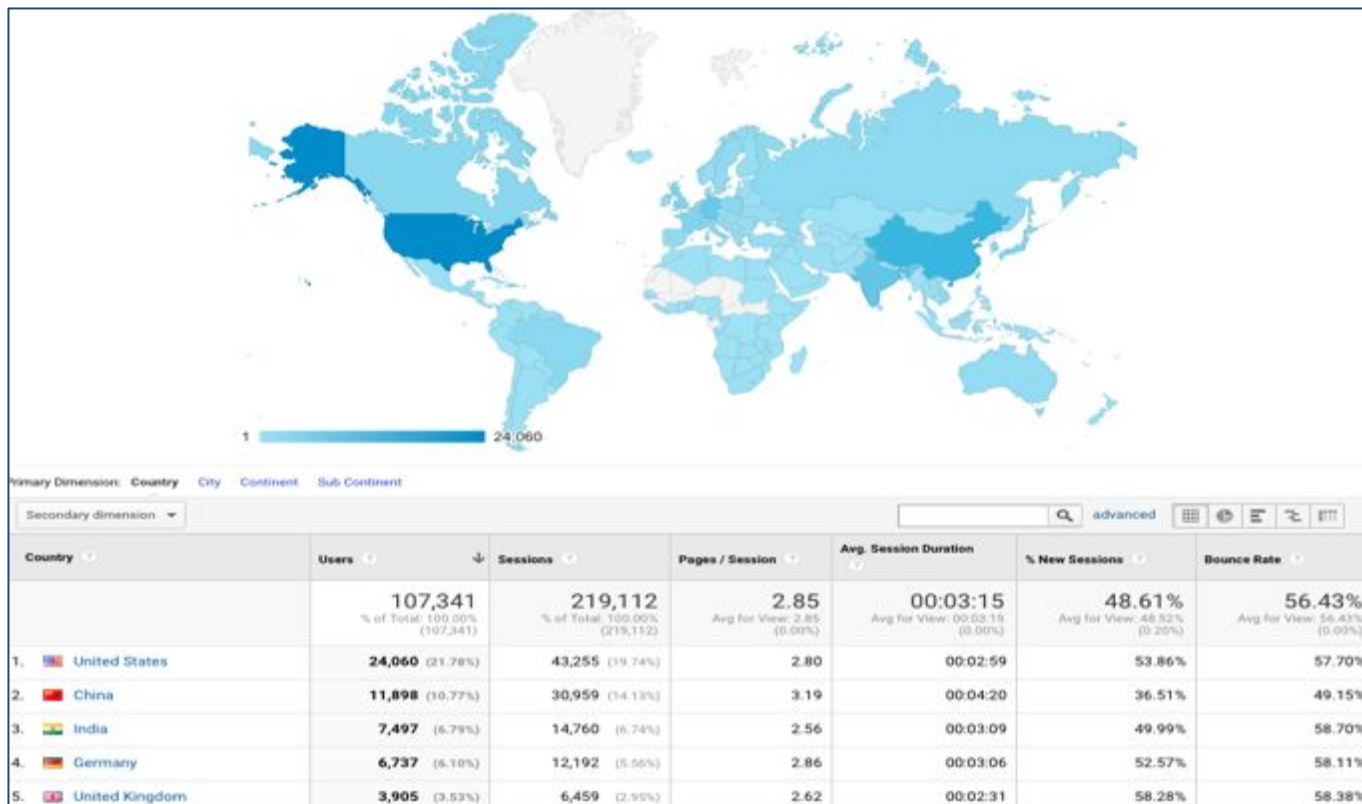
• 2016/2: 4
• 2020/7: 200+

Company Participation over the last 12 months



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

Zephyr.org Web Traffic in Last Year



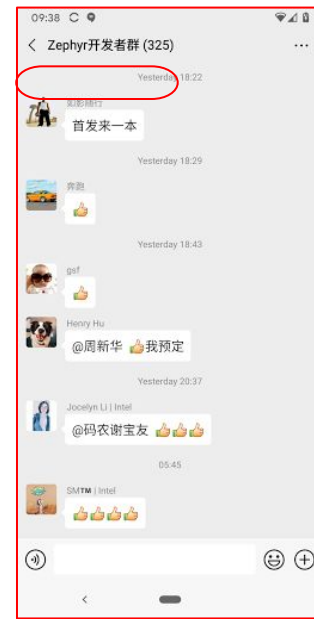
Vibrant, Active & Global Community



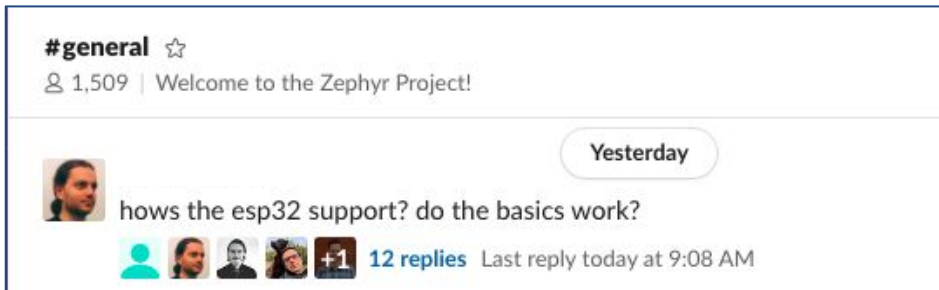
> 4300 Followers on Twitter



> 325 Members in WeChat Group



> 1500 Active on Slack



Zephyr Participation Information

Orientation:

- <https://www.zephyrproject.org/developer-resources/#how-to-contribute>
- <https://docs.zephyrproject.org/latest/contribute/index.html>

Github:

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

Mail Lists:

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

Slack:

- <https://tinyurl.com/y5glwylp>

Member Information

Join Today:

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

Why Become a Member?

- Industry Leadership
- Fast track to Technical Steering Committee Participation
- Help shape the Zephyr Certification Program
- Marketing Opportunities
- Member Networking Opportunities within the Zephyr Project
- Learning and Engagement

Meeting Schedule	
Technical Steering Committee	Weekly, Wednesdays
Marketing Committee	Bi-weekly, Mondays
Security Committee	Bi-Weekly, Thursday (members only)
Safety Committee	Bi-Weekly, Tuesday (members only)
Governing Board	Monthly (Platinum members only)



www.zephyrproject.org