

# Zephyr: Developing Open Source for **Safety and Security**

Kate Stewart, The Linux Foundation, @\_kate\_stewart

March 14, 2019



# Zephyr Project:

- **Open source** real time operating system
- **Vibrant Community** participation
- Built with **safety and security** in mind
- **Cross-architecture** with growing developer tool support
- **Vendor Neutral** governance
- **Permissively** licensed - Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**, better than roll-your-own
- **Product** development ready with LTS
- **Certification** ready with Auditable

Open Source, RTOS, Connected, Embedded  
Fits where Linux is too big

## Zephyr OS

3<sup>rd</sup> Party Libraries

Application Services

OS Services

Kernel

HAL

# Why Zephyr?

The Zephyr OS addresses broad set of embedded use cases across a broad set of platforms and architectures using a modular and configurable infrastructure. It addresses the need for RTOS consolidation.



## Address Fragmentation

- No single RTOS addresses broad set of embedded use cases across a broad set of platforms and architectures
- Disjoint use cases have led to fragmentation in RTOS space
- Existing commercial solutions force roll your own solutions and duplication of software components



## Modular Infrastructure

- Modular and configurable infrastructure allows creation of highly compact and optimal solutions for different products from a **common** origin
- Reuse allows NRE costs to be amortized across multiple products and solutions
- Multi-architecture support reduces platform switching costs and vendor lock-in concerns



## Open-Source

- Roll your own is expensive & difficult to develop & maintain
- Permissively licensed corresponds to ease of adoption
- Corporate sponsorship assures long term commitment and longevity
- Community innovation has proven faster for progression and project development is a collaboration of industry experts

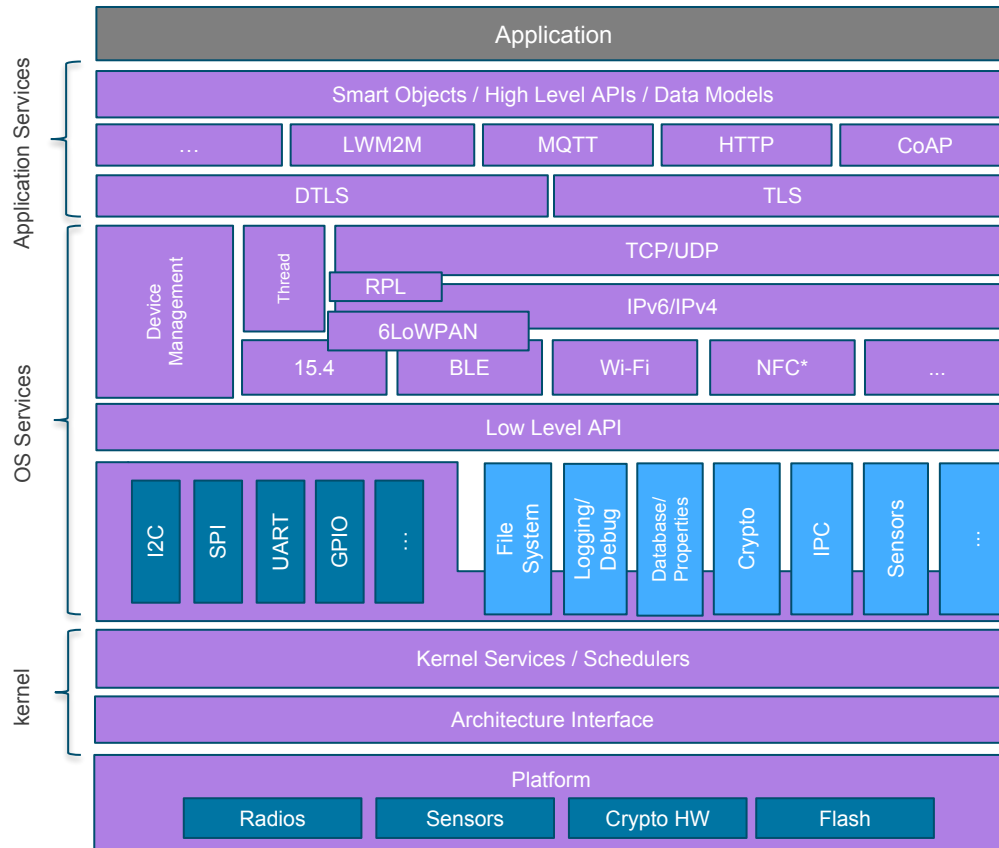


## Feature Richness

- Need for a solution rather than just an ingredient.
- Lowers entry level barrier for new products, speeds software delivery using existing feature support
- Encourages adherence to standards and promotes collaboration on complex features in the project
- Developers focus on the end-user facing interfaces instead of re-inventing low level interfaces

Reduce costs and improve efficiency through reuse

# Architecture



- Highly Configurable, Highly Modular
- Cooperative and Pre-emptive 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 4.2, 5.0) with both controller and host, BLE Mesh
- Native, fully featured and optimized networking stack

Fully featured OS allows developers to focus on the application

# Zephyr Ecosystem



## Zephyr OS

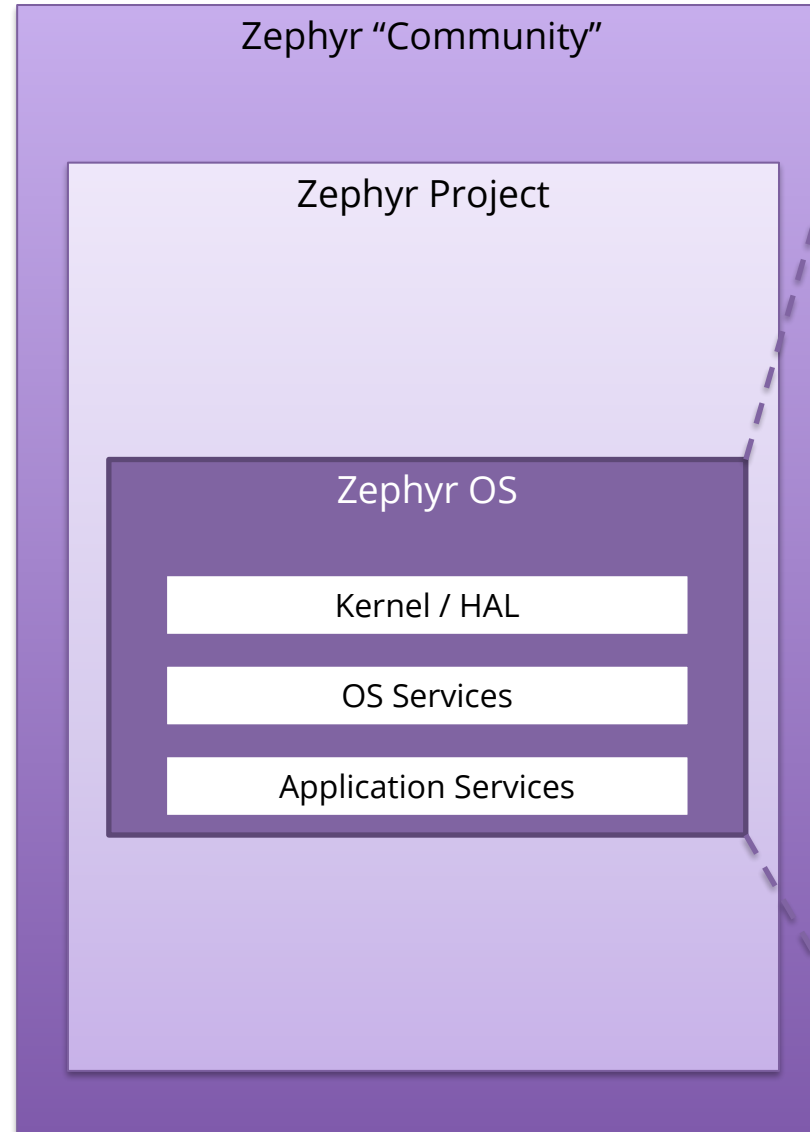
- The kernel and HAL
- OS Services such as IPC, Logging, file systems, crypto

## Zephyr Project

- SDK, 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: Jerryscript, Micropython, Iotivity



## Kernel / HAL

- Scheduler
- Kernel objects and services
- low-level architecture and board support
- power management hooks and low level interfaces to hardware

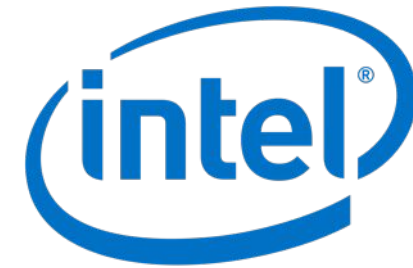
## OS Services and Low level APIs

- Platform specific drivers
- Generic implementation of I/O APIs
- File systems, Logging, Debugging and IPC
- Cryptography Services
- Networking and Connectivity
- Device Management

## Application Services

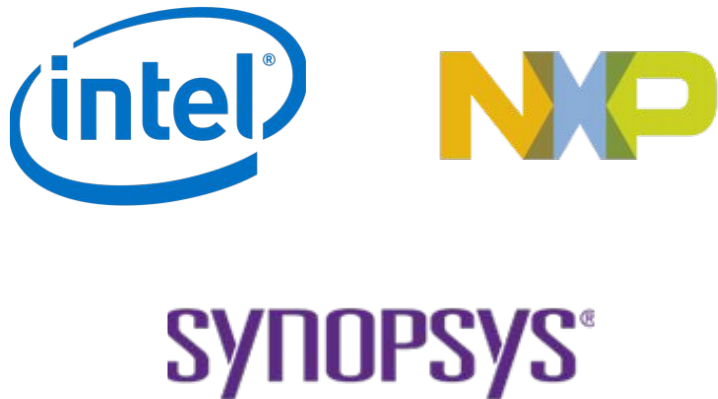
- High Level APIs
- Access to standardized data models
- High Level networking protocols

# Zephyr Supported Architectures



# Zephyr Project Membership

February 2016



SYNOPSYS®

February 2019



SYNOPSYS®



and others....



# Sample of Board Support



SiFive HiFive1



Arduino Due



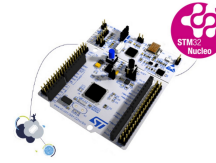
Nucleo 103RB



NRF51



Nucleo64 L476RG



Nucleo F411RE



NRF52 pca10040



Nucleo F334R8



Synopsys EMSK



Arduino 101



Minnowboard



Altera MAX10



Nucleo 401RE



Hexiwear



ARM V2M MPS2



STM3210c



Atmel SAM E70



Adafruit Feather



Galileo



NXP FRDM K64F



NRF52



Seed Carbon



TI Launchpad Wifi



BBC Microbit



STM32373c



Redbear BLE Nano



96b Neon Key



Quark D2000



STM32 Olimexino



STM Mini A15



Seed Nitrogen



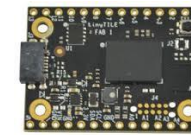
ARM V2M Beetle



Zedboard Pulpino



NXP FRDM-KW41Z



tinyTILE



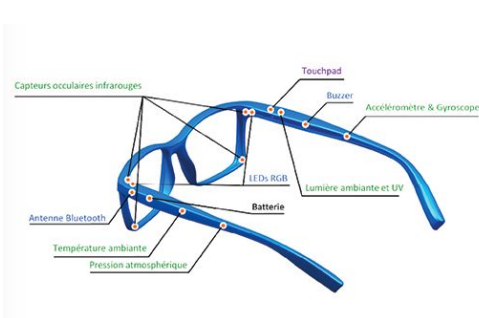
NXP i.MX RT1050

**141 BOARDS** TODAY WITH MORE ON WAY...

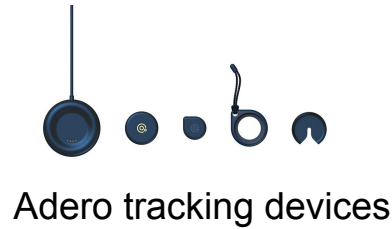
<http://docs.zephyrproject.org/boards/boards.html>



# Products Running Zephyr Today



Ellcie-Healthy Smart Connected Eyewear



Rigado IoT Gateway



ProGlove Scanning Gloves



GNARBOX 2.0 SSD



Antmicro Badge



Grush Gaming Toothbrush



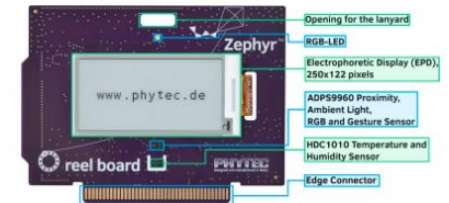
hereO Smartwatch



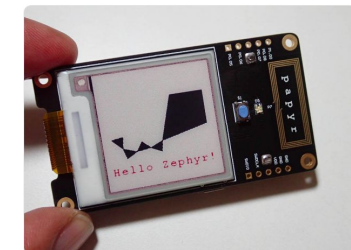
Blocks Modular Smartwatch



Intellinium Safety Shoes



Reel Board



Papyr

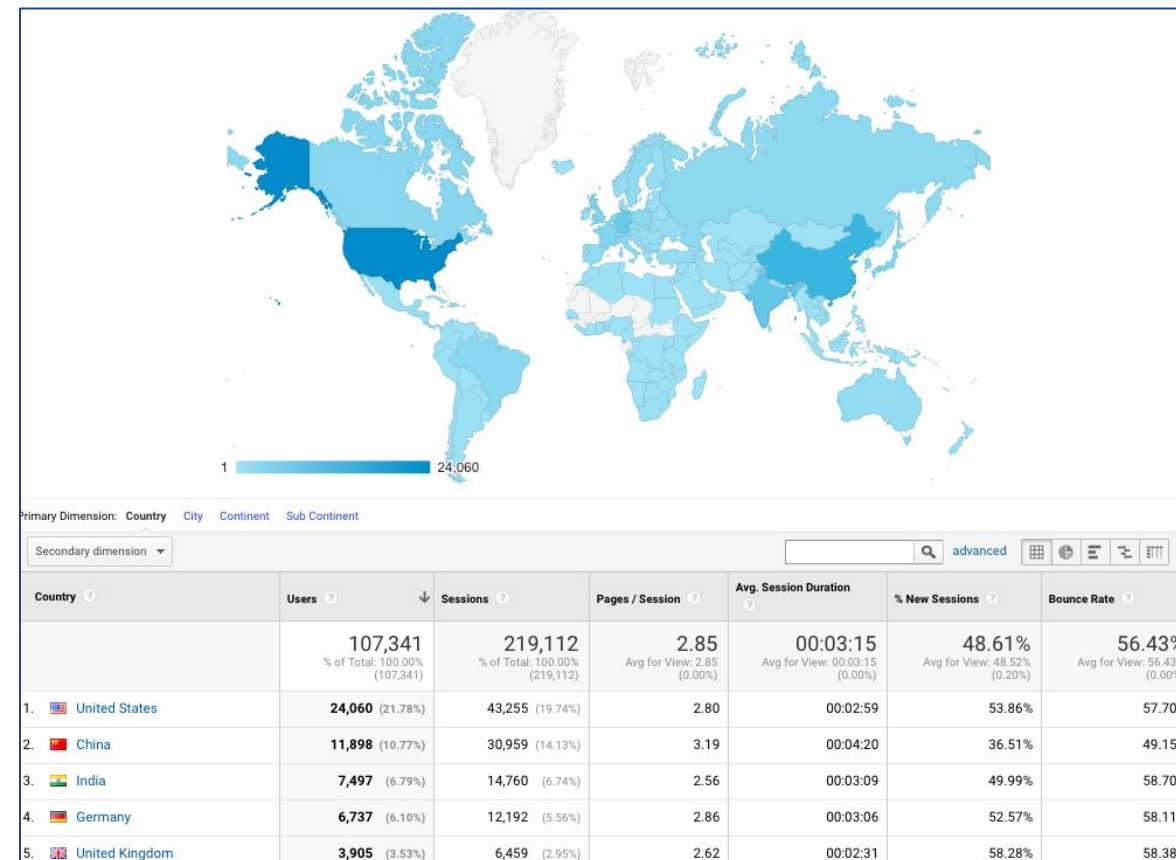
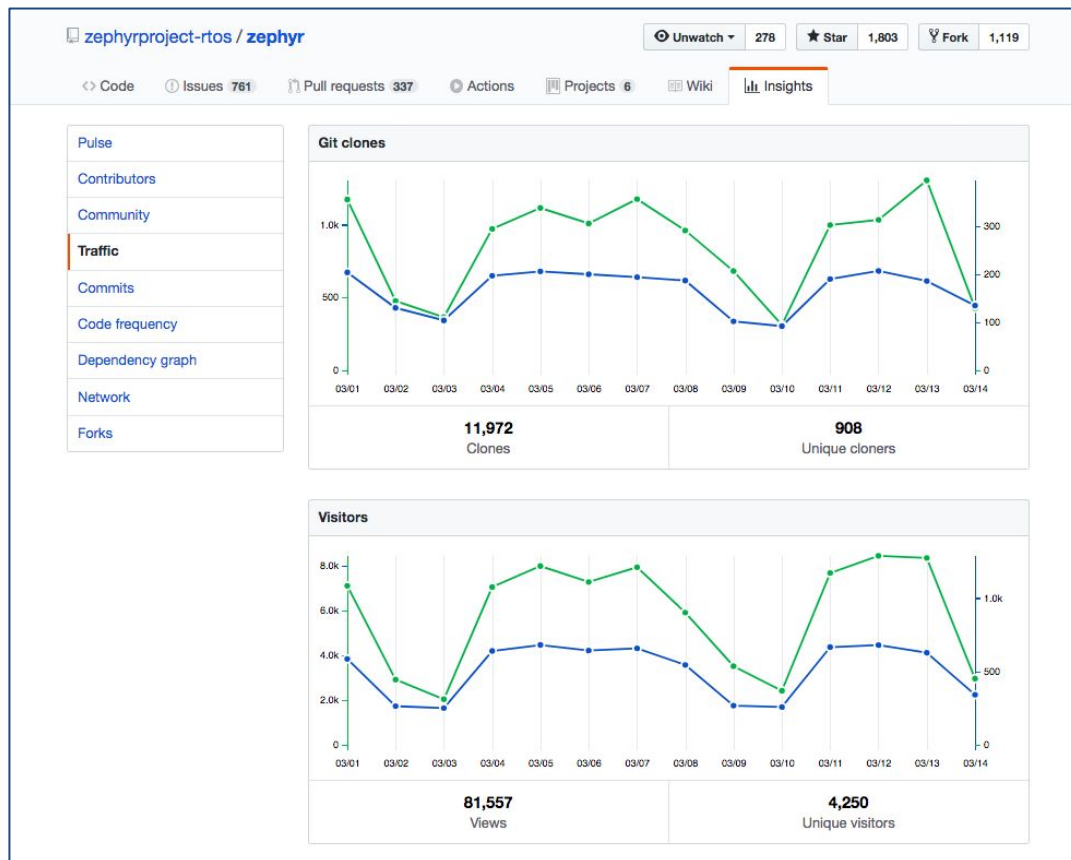
# Growing a Diverse Community!



## 1.13 release statistics:

- › 13 weeks cycle, with 2 weeks of merge window
- › 1,834 changes (patch commits)
- › 140 developers identified
- › 25 companies participated
- › 20 changes / day ( .8/hour)

# Vibrant & Distributed Community



# Developer Tools...



RENODE™

by:  antmicro  
EMBEDDED SYSTEMS



Synopsys  
DesignWare  
ARC Development  
Tools





# Zephyr Project:

- **Open source** real time operating system
- **Vibrant Community** participation
- Built with **safety and security** in mind
- **Cross-architecture** with growing developer tool support
- **Vendor Neutral** governance
- **Permissively** licensed - Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**, better than roll-your-own
- **Product** development ready with LTS
- **Certification** ready with Auditable

Open Source, RTOS, Connected, Embedded  
Fits where Linux is too big

## Zephyr OS

3<sup>rd</sup> Party Libraries

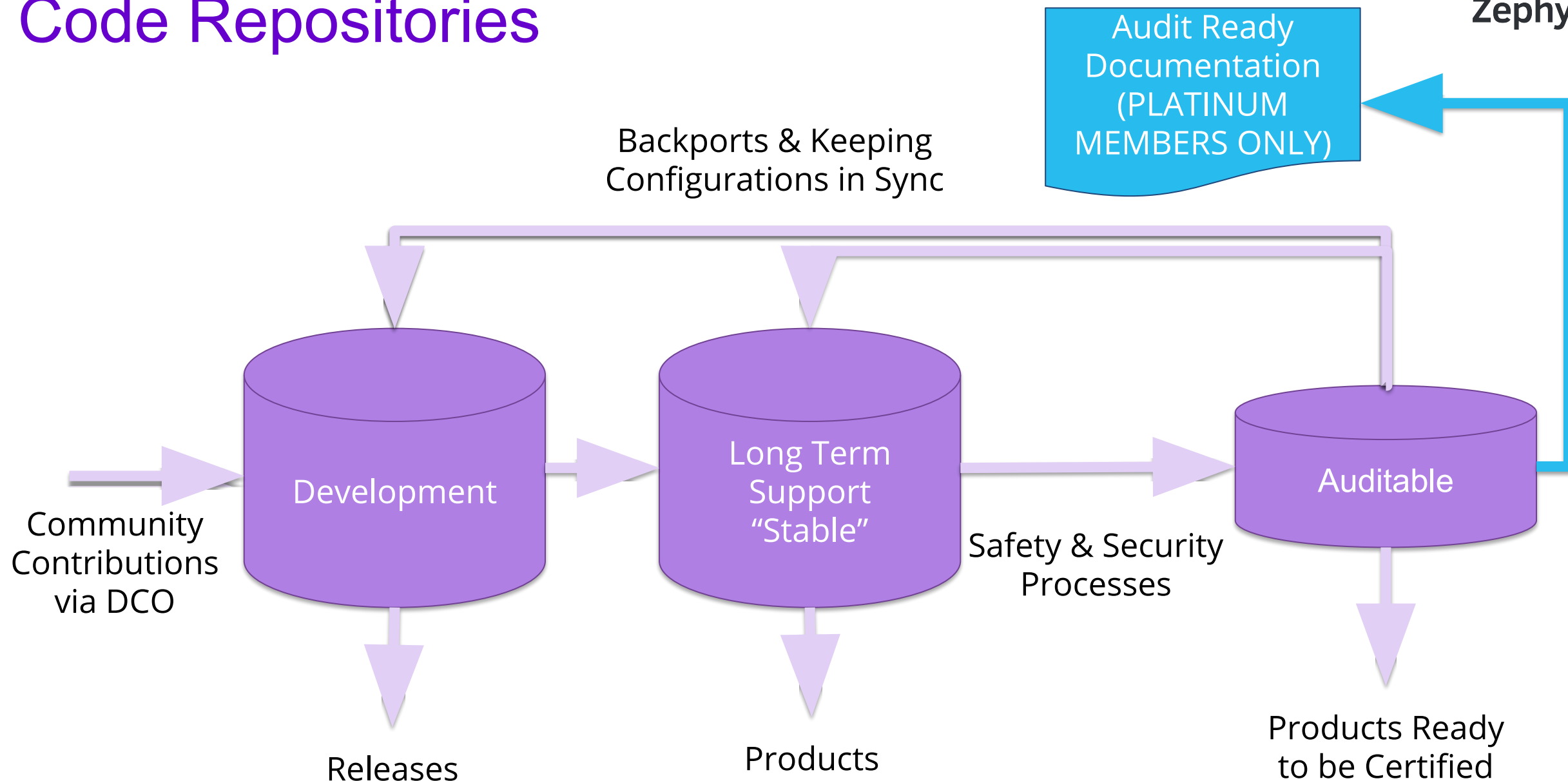
Application Services

OS Services

Kernel

HAL

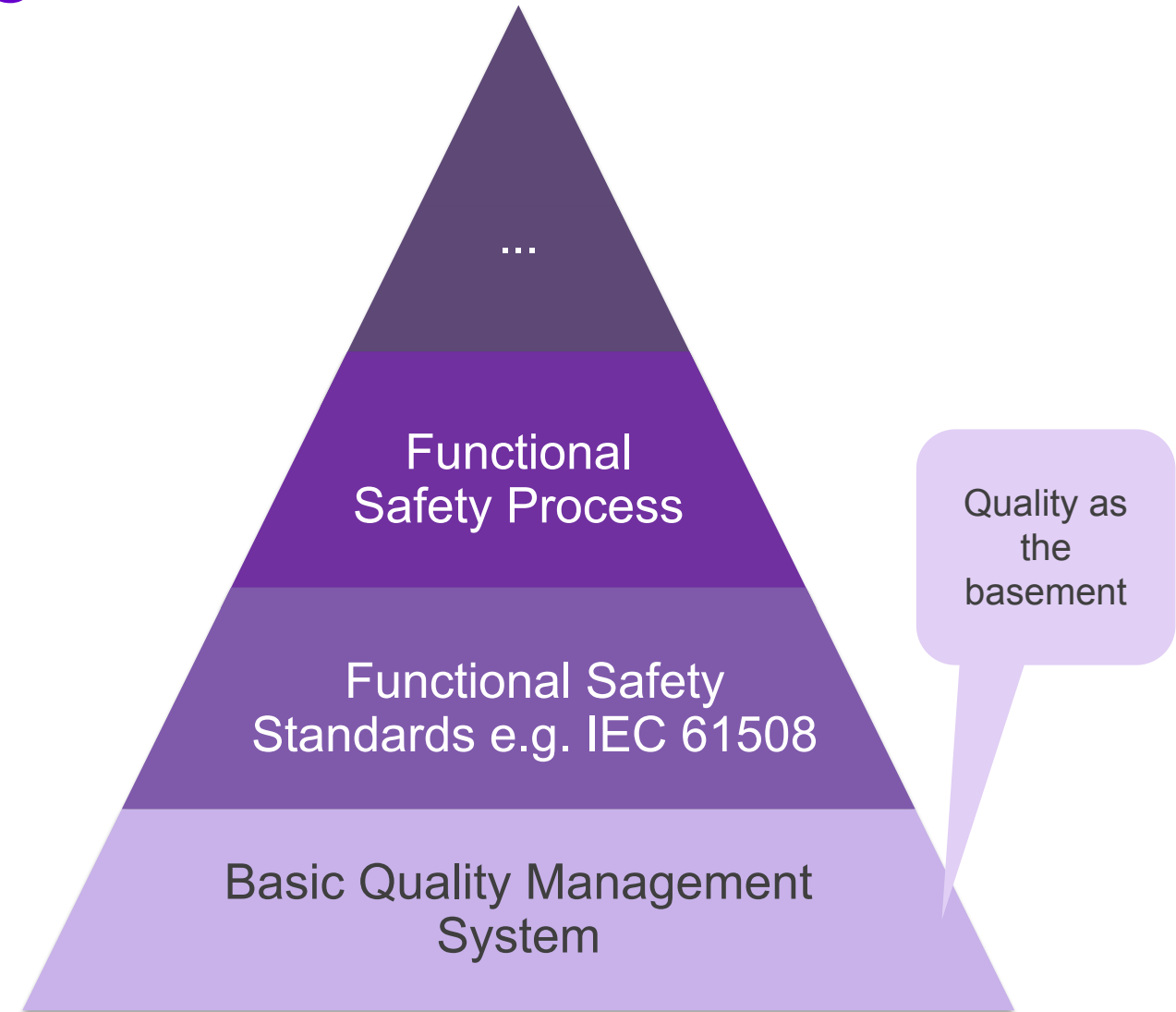
# Code Repositories





# Zephyr OS: Quality Matters

- 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: Long Term Support (LTS)

## It is:

- **Product Focused**
- **Compatible with New Hardware:** We will make point releases throughout the development cycle to provide functional support for new hardware.
- **More Tested:** Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- **Certifiable:** The base for the auditable branch


## It is not:

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

# Zephyr OS: Preparation for Auditable


- Established Security Working Group, 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.

# CII Badge Status:


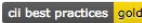
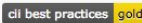

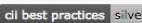

**CII Best Practices**

[Projects](#)
[Sign Up](#)
[Login](#)

**2167 Projects**

Badge status: All
 Exclude passing: ☐
 Text search: 


[Add New Project](#)


Id	Name	Description	Website	License	Owner	Last achieved at	Tiered %	Badge
126	<a href="#">league/commonmark</a>	Markdown parser for PHP based on the CommonMark spec.	<a href="https://github.com/t-hephpleague/commonmark">https://github.com/t-hephpleague/commonmark</a>	BSD-3-Clause	Colin O'Dell	2017-12-13 15:32:16	300%	
74	<a href="#">Zephyr Project</a>	The Zephyr Project is a small, scalable real-time operating system for use on resource-constrained systems supporting multiple architectures. Developers are...	<a href="https://www.zephyrproject.org">https://www.zephyrproject.org</a>	Apache-2.0	Brett Preston	2018-03-10 20:50:26	300%	
1	<a href="#">BadgeApp</a>	BadgeApp is the web application that allows developers to provide information about their project and (hopefully) get a Core Infrastructure Initiative (CII)...	<a href="https://github.com/coreinfrastructure/best-practices-badge">https://github.com/coreinfrastructure/best-practices-badge</a>	MIT	David A. Wheeler	2016-01-12 22:55:00	300%	
34	<a href="#">Linux Kernel</a>	The Linux kernel.	<a href="https://www.kernel.org">https://www.kernel.org</a>	GPL-2.0	Greg Kroah-Hartman	2018-06-14 16:10:57	296%	
1351	<a href="#">TUF (The Update Framework)</a>	A framework for securing software update systems.	<a href="https://www.theupdateframework.com">https://www.theupdateframework.com</a>	Apache-2.0 and MIT	David A. Wheeler	2017-11-20 19:26:07	274%	






## 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 a Core Infrastructure Initiative (CII) badge. [Show details](#)

If this is your project, please show your badge status on your project page! The badge status looks like this:  Here is how to embed it: [Show details](#)

These are the  level criteria. You can also view the  or  level criteria.

Basics	5/5
Change Control	4/4
Quality	7/7
Security	5/5
Analysis	2/2

1 of only 3 Golds in the 2,167 projects publicly documenting their practices!

# Zephyr OS: Auditable Code Base

Subset of ZephyrOS kernel derived from LTS code base.

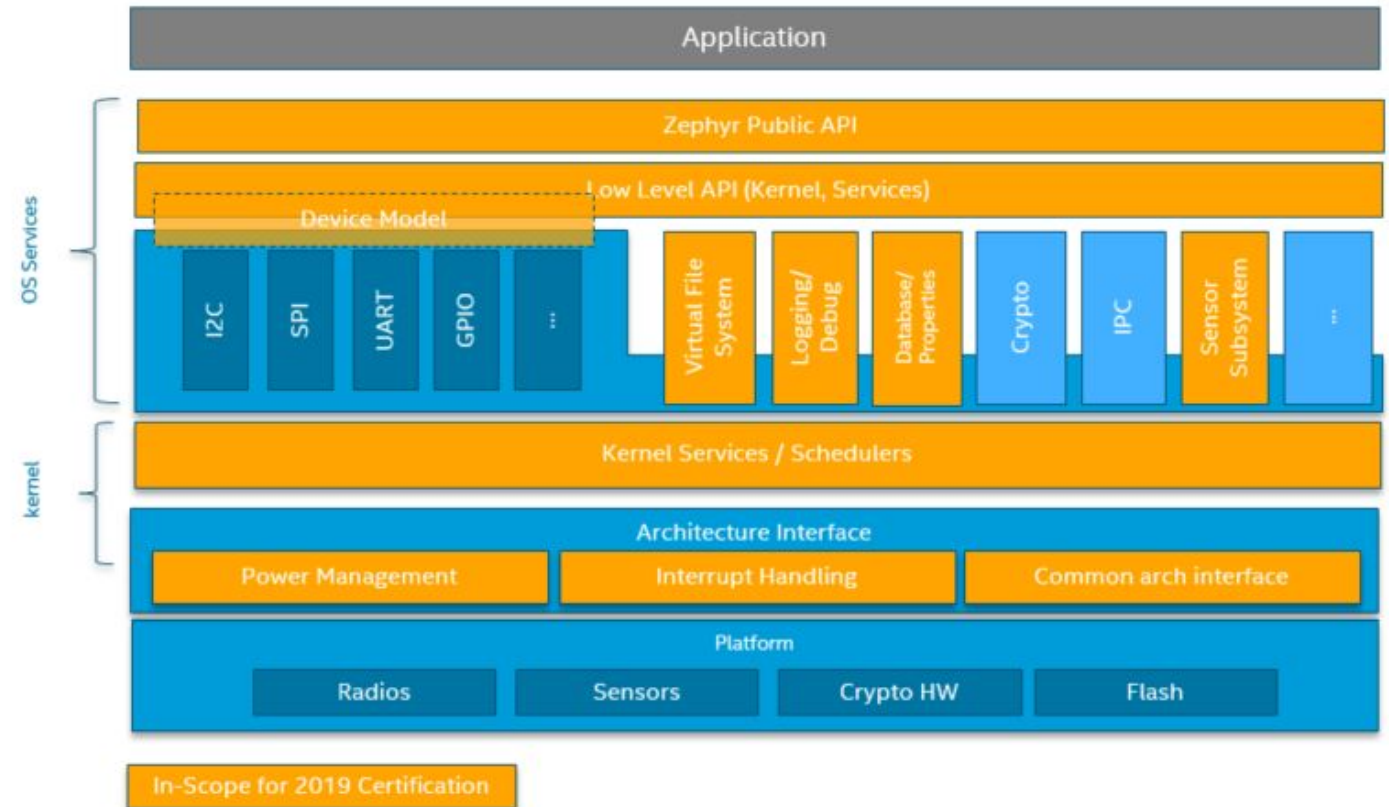
- Initial and subsequent certification targets to be decided by Governing Board.
- An auditable code base will be established from a subset of Zephyr OS.
  - Code bases will be kept in sync from that point forward.
  - More rigorous processes (necessary for certification) will be applied before new features move into the auditable code base.

Processes to achieve selected certification to be determined by Security Working Group and coordinated with Technical Steering Committee.

# 2019 Certification Scope (in orange)

Not in scope:

- Platform drivers or BSPs
- No platform specific power management implementation, only device and kernel part of PM.
- No Filesystem or sensor driver implementation, only interface and infrastructure to support those on top of existing APIs



See:

<https://www.zephyrproject.org/zephyr-project-rtos-first-functional-safety-certification-submission-for-an-open-source-real-time-operating-system/> for more details



# Zephyr OS: Candidate Standards

## Coding for Safety, Security, Portability and Reliability in Embedded Systems:

- [MISRA C:2012](#), with [Amendment 1](#), following [MISRA C Compliance:2016](#) guidance

## Safety:

- [IEC 61508: 2010](#)
  - broadest for robotics and autonomous vehicle engineering companies. Reference for other standards in Robotics domain.
  - [Sampled Certifications derived from IEC 61508:](#) Auto: ISO 26262; Medical: IEC 62304;

## Security:

- [Common Criteria](#) (EAL4 but possibly higher levels EAL5,6 )

## Others:

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

# Zephyr Developer Participation Information

## Orientation:

- <https://www.zephyrproject.org/community/how-to-contribute>
- [https://www.zephyrproject.org/doc/contribute/contribute\\_guidelines.htm](https://www.zephyrproject.org/doc/contribute/contribute_guidelines.htm)

## Github:

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

## Mail Lists:

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

## IRC:

- #zephyrproject on freenode.net

## Slack:

- <https://zephyrproject.slack.com> (get invite from github page)

# Member Information

**Join Today:** <https://www.zephyrproject.org/join/>

## Why Become a Member?

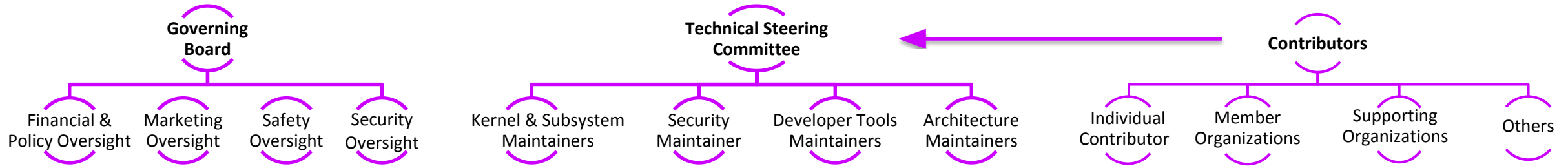
- Industry Leadership
- Fast track to Technical Steering Committee Participation
- Help shape the Zephyr Certification Program
- Marketing Opportunities
- Member Networking Opportunities within the Zephyr Project
- Learning and Engagement

Meeting Schedule	
Technical Steering Committee	Weekly, Wednesdays
Marketing Working Group	Bi-weekly, Mondays
Security Working Group	Bi-Weekly, Wednesdays (members only)
Governing Board	Monthly (members only)



[www.zephyrproject.org](http://www.zephyrproject.org)

# Zephyr Project Governance



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

## Governing Board

- Decides project goals
- Sets 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