2019年中国嵌入式技术大会
EMBEDDED TECHNOLOGY
Conference China 2019

ETCC

SYNOPSYS®
Silicon to Software™

Zephyr: an Open Source RTOS for AIoT

Wayne Ren (任慰)

2019-12-19

Agenda

- Zephyr overview
- Zephyr’s architecture
- Zephyr’s secure/safe
- Zephyr in Synopsys

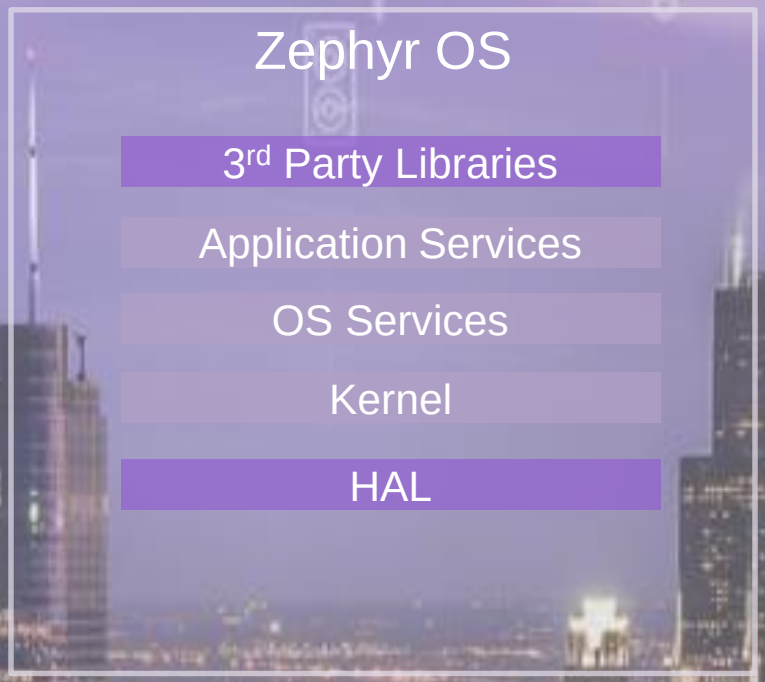
Zephyr overview

Zephyr Project:

- Started in 2016 by Intel, Synopsys, NXP
- **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

THE LINUX FOUNDATION PROJECTS

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



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

Zephyr Project Members

Zephyr’s Vibrant Community (2019/10/24)

Total Contributors

Rank	RTOS	#
1	**Zephyr**	**559**
2	Mbed OS	552
3	nuttX	344

Total Commits

Rank	RTOS	#
1	nuttX	39,978
2	**Zephyr**	**34,571**
3	mbed OS	27,034

Zephyr Supported Hardware Architectures

ARC Synopsys · arm · intel · RISC-V · tensilica (xtensa)


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


Seeed Carbon


TI Launchpad Wifi


BBC Microbit


STM32373c


Redbear BLE Nano


96b Neon Key


Quark D2000


STM32 Olimexino


STM Mini A15


Seeed Nitrogen


ARM V2M Beetle


Zedboard Pulpino

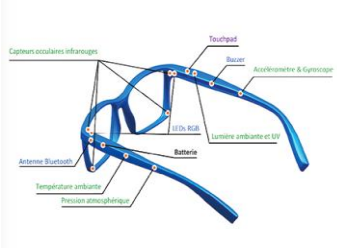

NXP FRDM-KW41Z


tinyTILE


NXP i.MX RT1050

200+ BOARDS TODAY WITH MORE ON WAY…
http://docs.zephyrproject.org/boards/boards.html

Products Running Zephyr Today



Ellcie-Healthy Smart Connected Eyewear

Rigado IoTGateway

ProGlove Scanning Gloves

Adero tracking devices

RUUVI node

GNARBOX 2.0 SSD

GEPS

Point Home Alarm

Grush Gaming Toothbrush

hereO Smartwatch

Intellinium Safety Shoes

Anicare reindeer tracker

HereO Core Box

Zephyr's 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

What's New

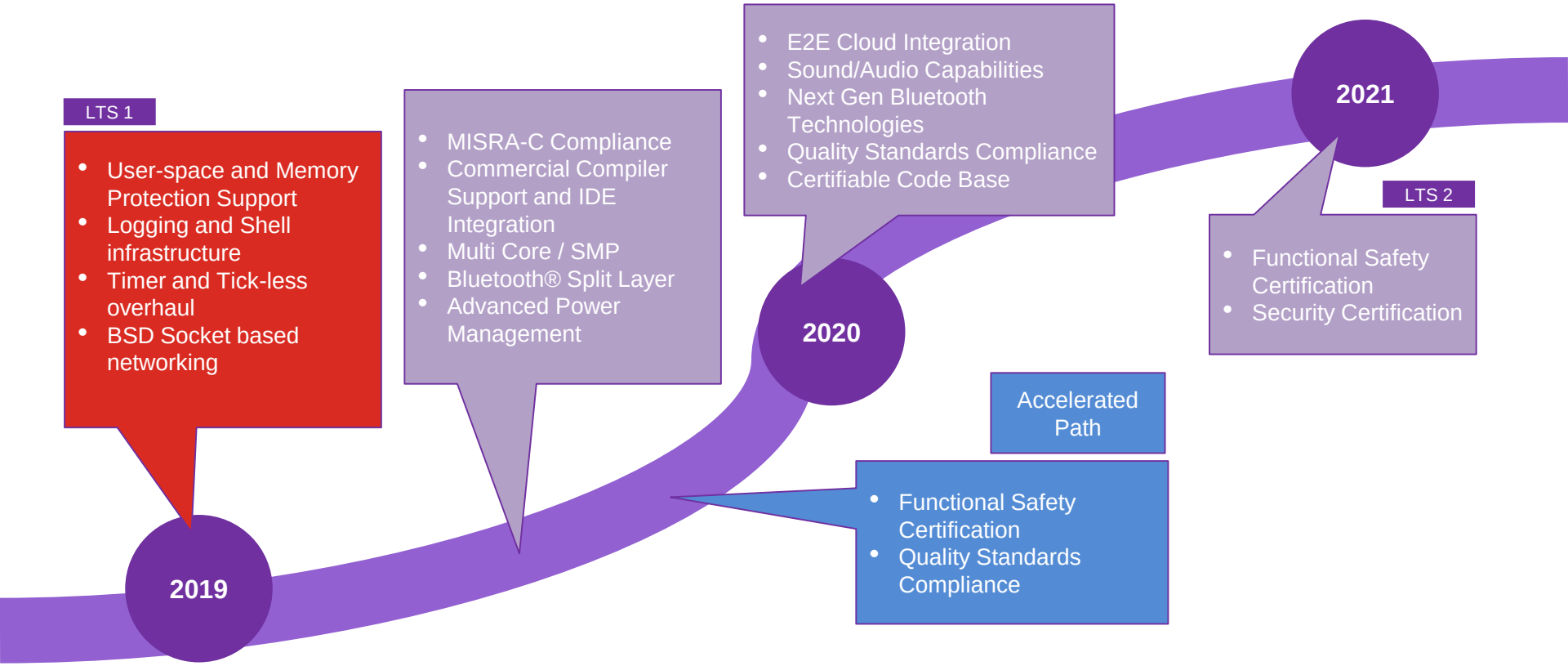
Release per 3 months, Long Term Support(LTS) release per 2 years

- Zephyr 1.14 LTS
  - 6 month development cycle, a Major Technical Milestone, baseline for the auditable branch
  - **Product Focused**
  - **Current with latest Security Updates**
  - **More Tested**
  - Zephyr 1.14.1 is released

- Zephyr 2.1 (2019.12.09)
  - Normalized APIs across all architectures
  - Support for numerous new boards, shields, drivers and sensors
  - Expanded support for ARMv6-M architecture
  - Added new TCP stack implementation
  - Memory size improvements to Bluetooth host stack

- Zephyr 2.2 will be 2020.02.28

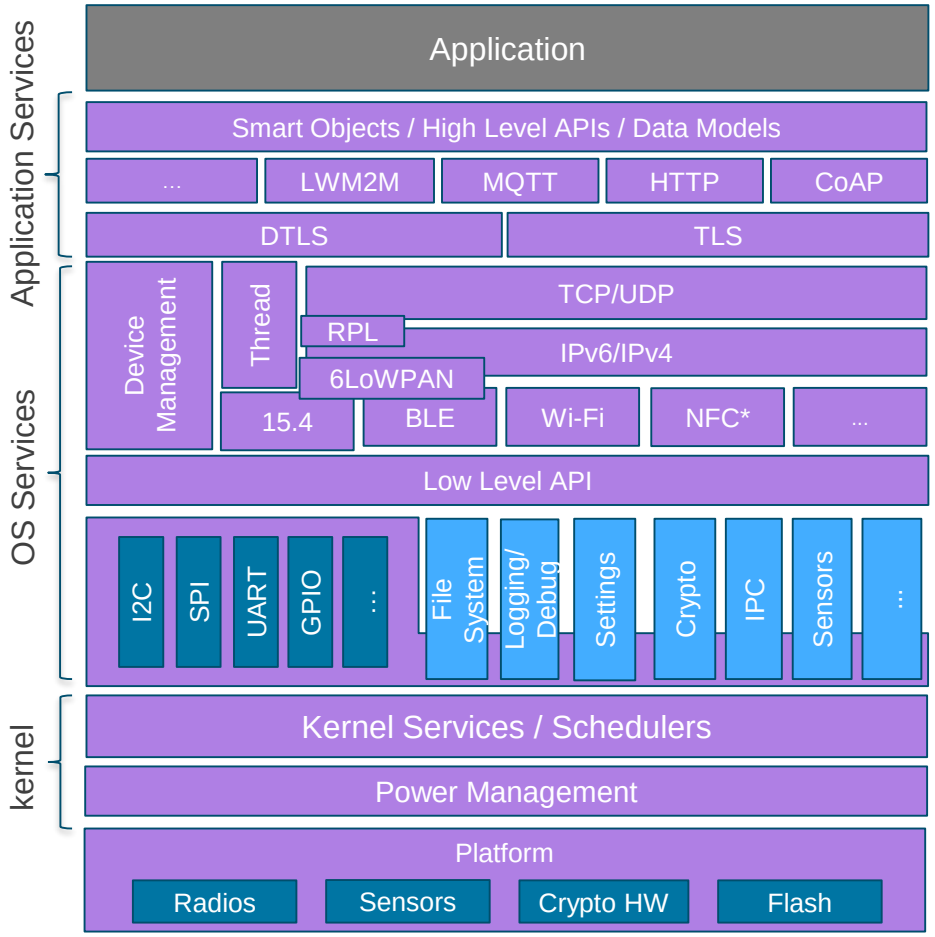
Zephyr Project Roadmap



Zephyr architecture

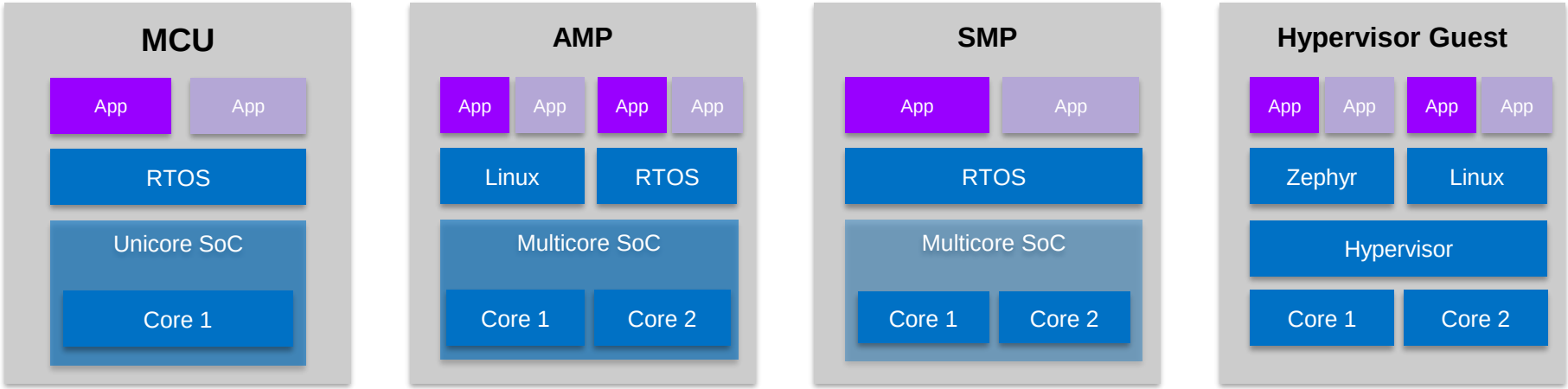
Architecture

- 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
- 802.15.4 OpenThread
- Native, fully featured and optimized networking stack



Fully featured OS allows developers to focus on the application

System Configurations



Single Core MCU

Supported with OpenAMP

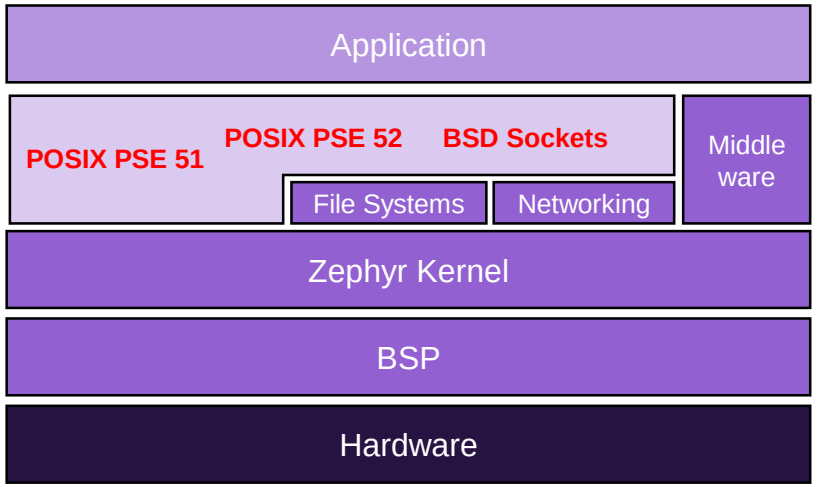
Supported on some architectures

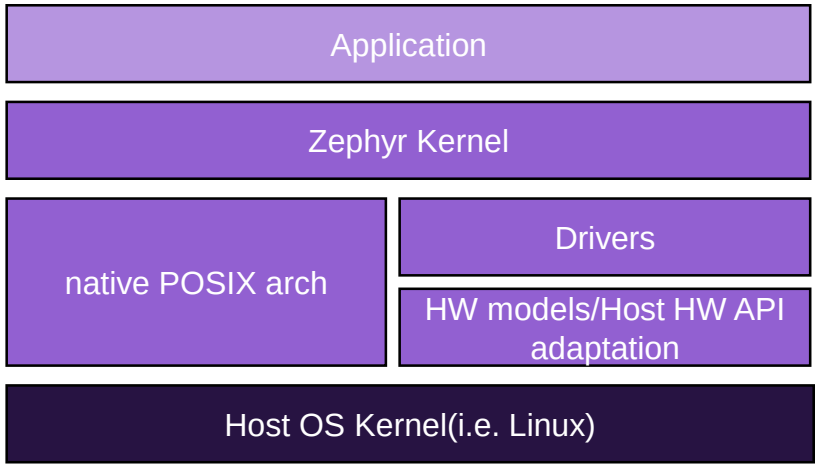
Supported with ACRN

Safety and security can apply to all these configurations

POSIX support

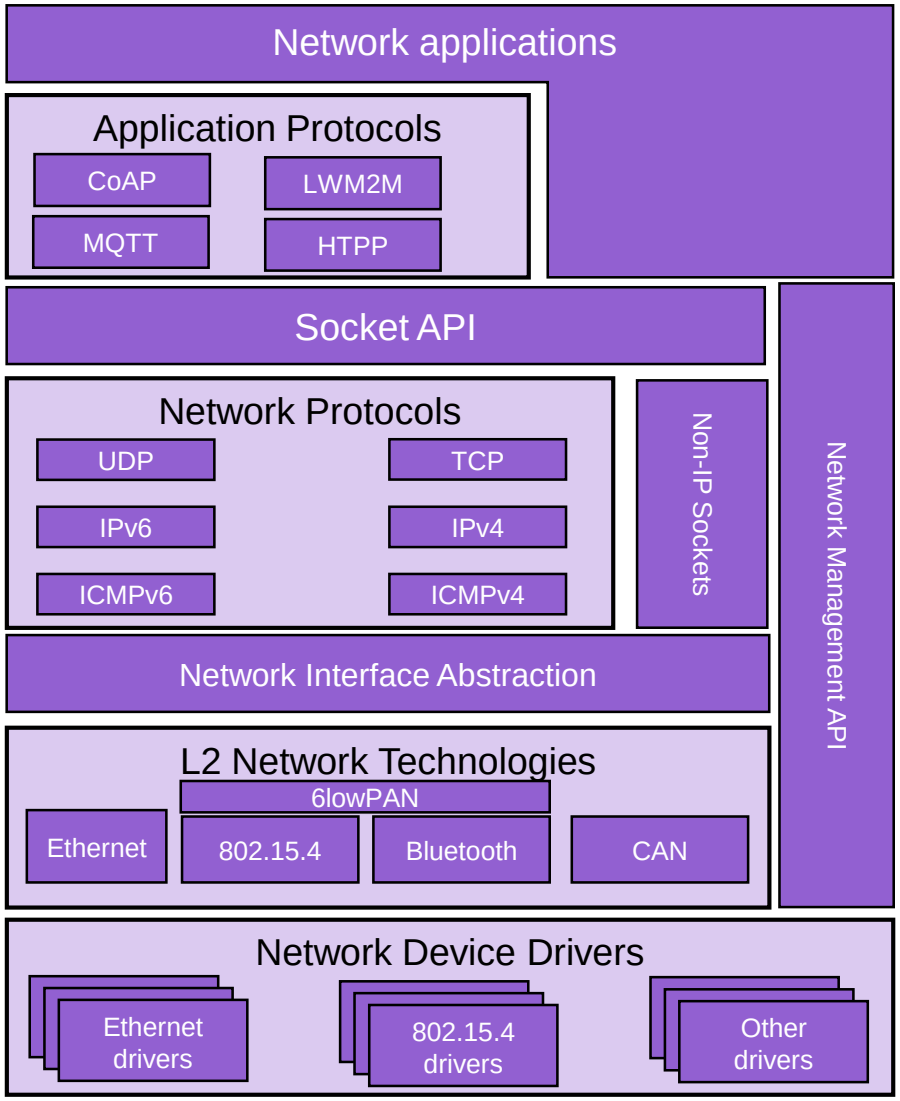
- POSIX API
  - Provides familiar APIs to non-embedded programmers, especially to Linux developers
  - Enables re-use (portability) of existing libraries based on POSIX APIs
  - Provide efficient subset appropriate for small (MCU) embedded systems
  - POSIX API subset is increasingly popular operating system abstraction layer (OSAL) for IoT
  - Supports subsets of PSE51, PSE52 and BSD Sockets API
- Native execution on a POSIX OS
  - Enable large scale simulation of network or Bluetooth tests without involving hardware
  - 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 hardware test platforms during development





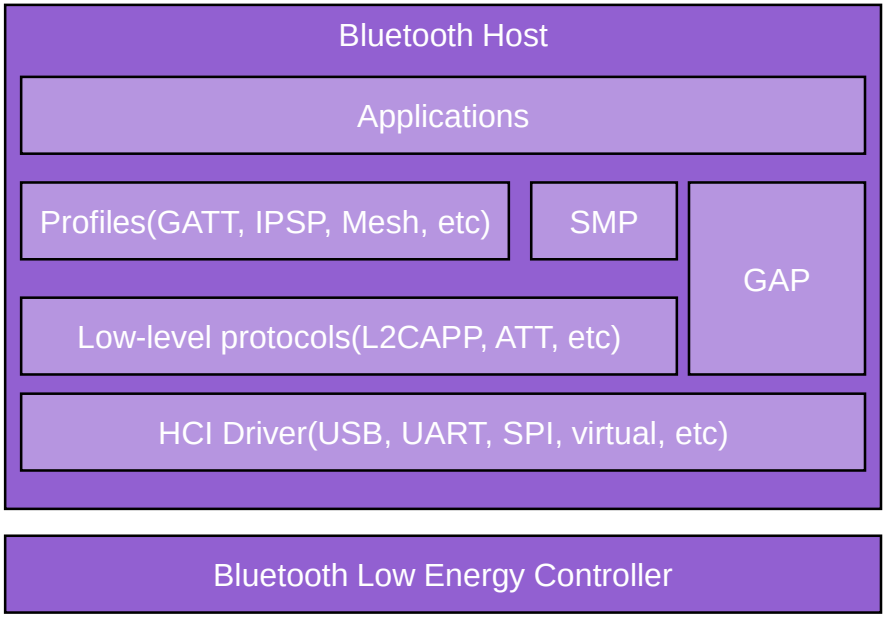
Native IP Stack

- Built 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
- 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

- 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

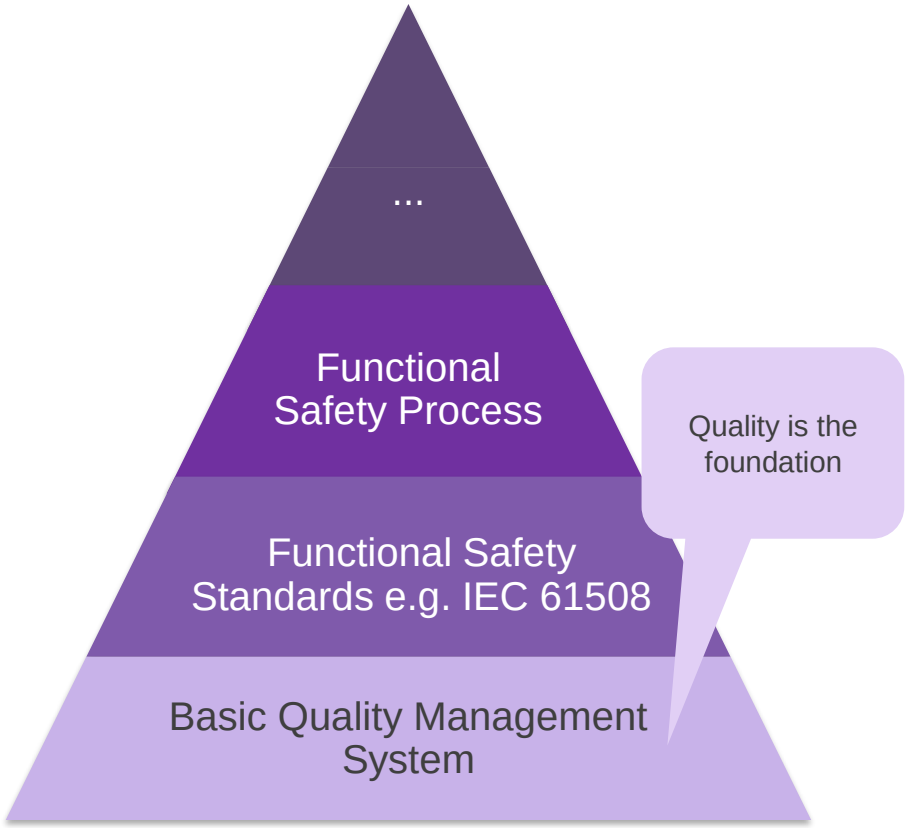


- Bluetooth Low Energy Controller
  - 2nd generation open source implementation
  - Split design with Upper and Lower Link Layers
  - Support for multiple Bluetooth LE radio hardware architectures
    - Nordic nRF5 Series on ARM Cortex-M
    - VEGA board on RISC-V
  - Asynchronous handling of procedures 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

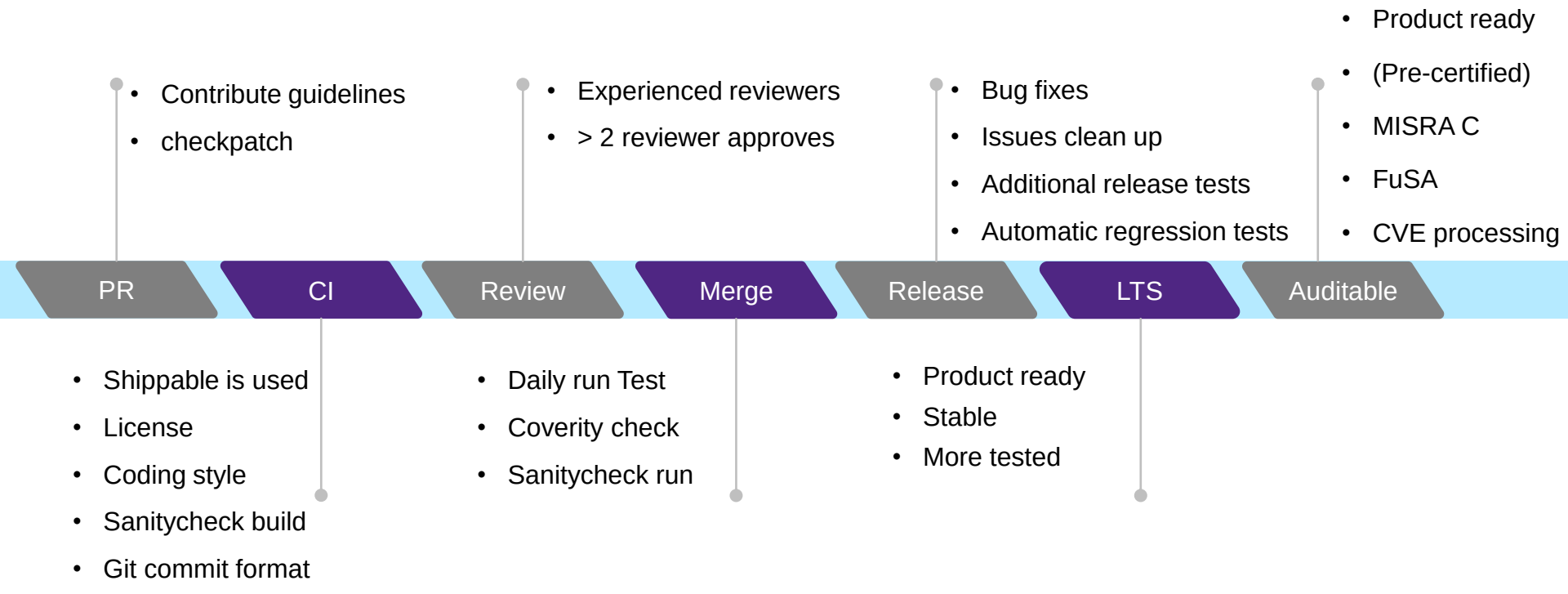
Zephyr’s secure and safe Design

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**



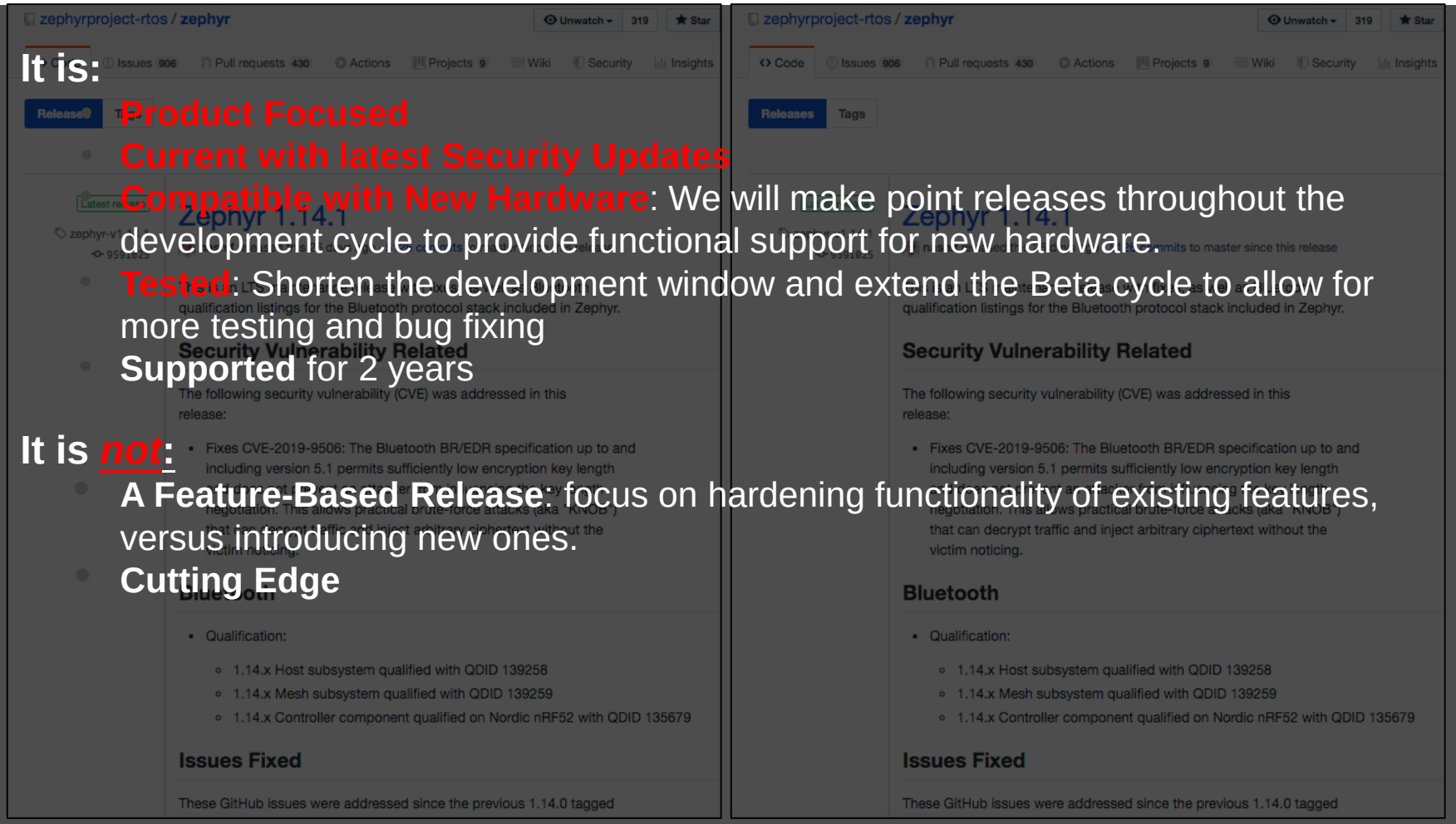
Zephyr Development Flow



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**
- Passing 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: Long Term Support (LTS)



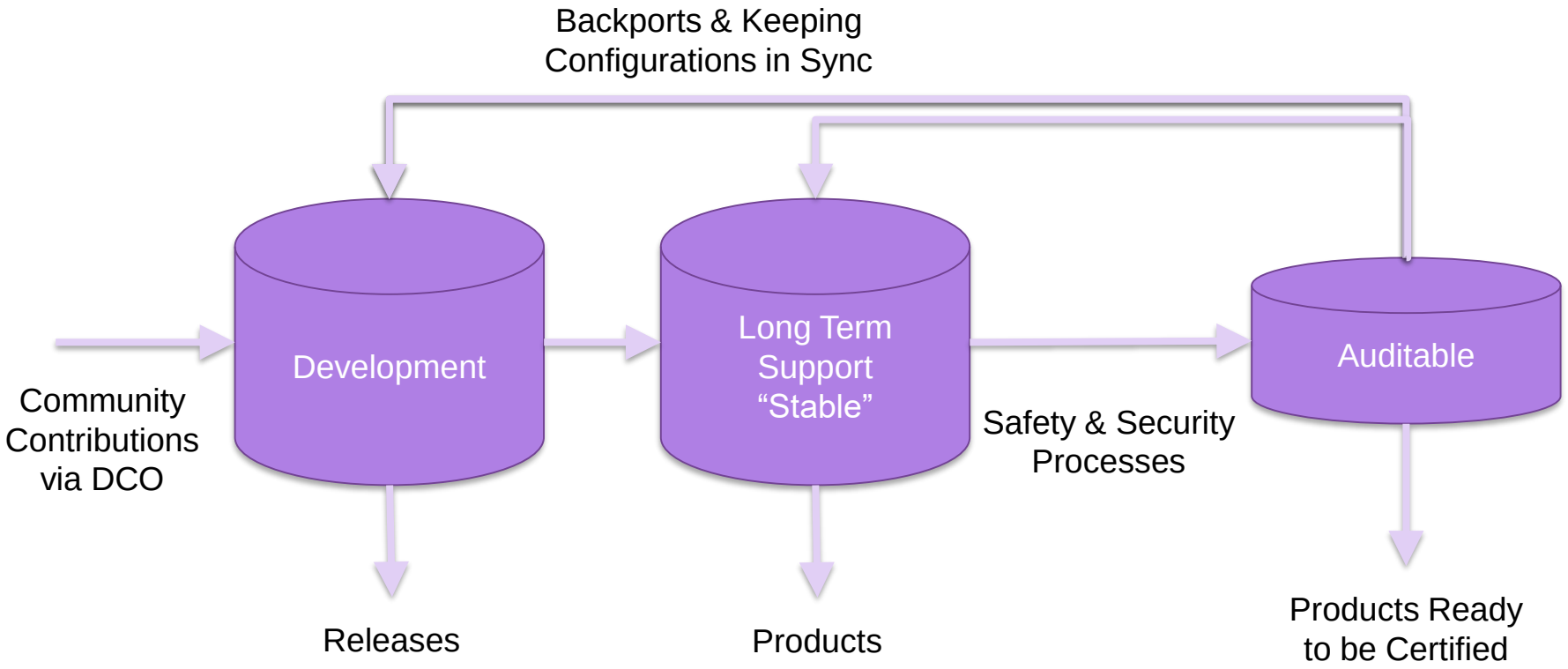
It is:

- **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**

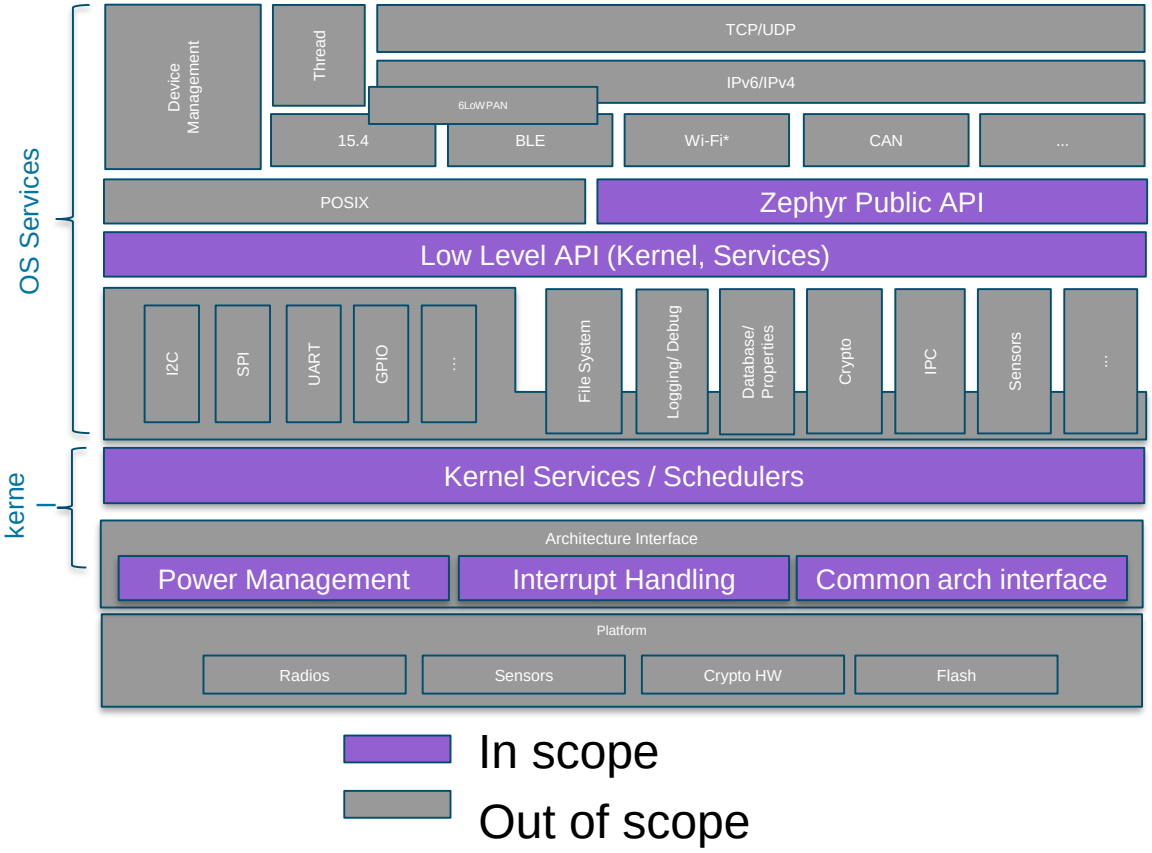
Code Repositories



2019 Auditable Scope

Not in scope:

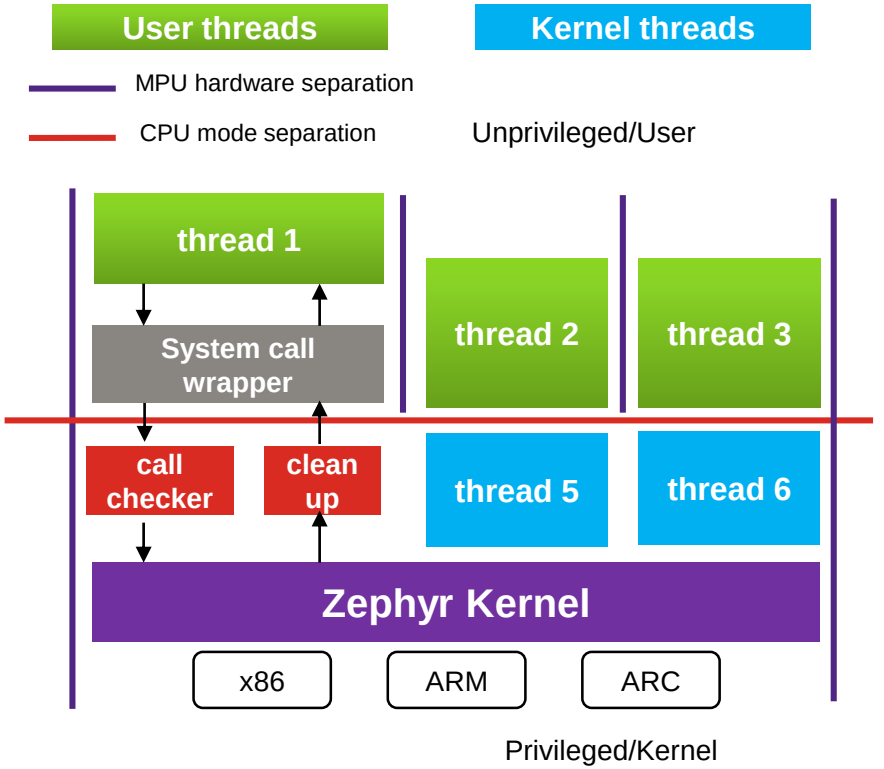
- Platform drivers or BSPs
- No platform specific power management implementation, only device and kernel part of power-management
- No filesystem or sensor driver implementation, only interface and infrastructure to support those on top of existing APIs



User Space in Zephyr

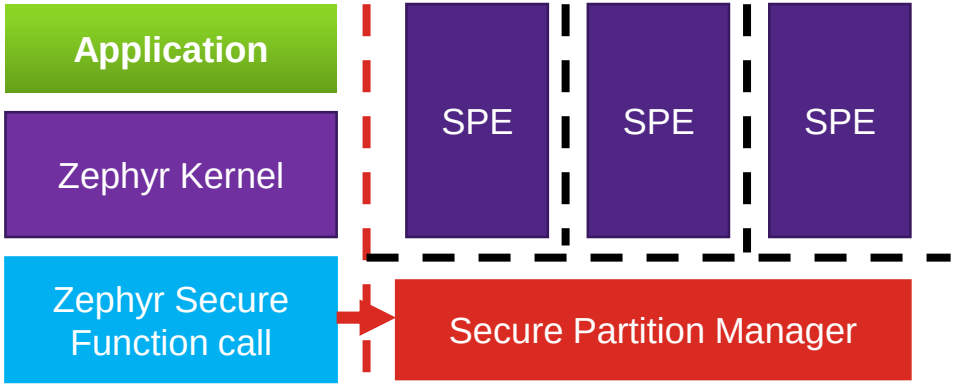
RTOS supporting user space are few

- User thread
  - Untrusted
  - Isolated from the kernel and each other
- Kernel thread and kernel
  - Trusted, privilege to access all resources
  - Drivers, network stack etc. are in kernel
- A flawed or malicious user thread cannot:
  - Leak or modify private data of another thread unless specifically granted permission
  - Interfere with or control another thread except through designed thread communication APIs (pipes, semaphores, etc.)
- System call
  - API ID and parameters are marshaled into registers and a software interrupt/exception is triggered
  - Validate API ID in checker, clear regs on exit
  - Use build-time logic to make adding new system calls as painless as possible

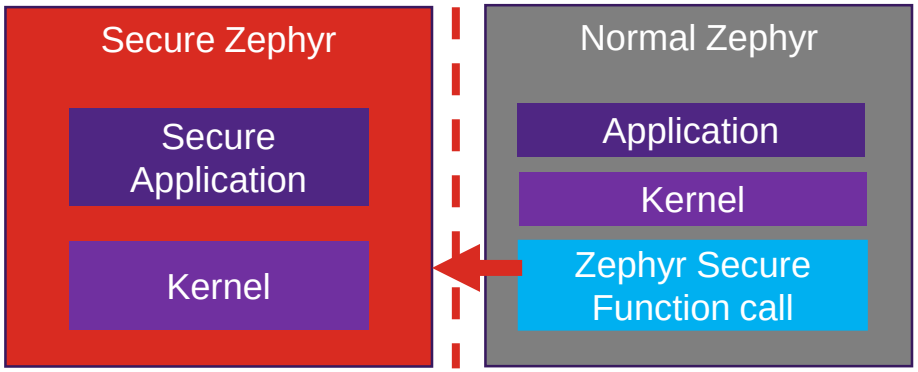


Zephyr and TEE(Trust Execution Environment)

- TEE for Microcontrollers
  - Synopsys ARC SecureShield™
  - ARM Trust-Zone M
- TEE in Zephyr
  - ARM
    - ARMv8m supported (Cortex M23/M33)
    - Needs ARM TFM (ARM Trusted Firmware for Cortex M)
    - Zephyr is an application of TFM
  - ARC (Zephyr 2.0)
    - Two worlds, two binary, secure Zephyr run first, normal Zephyr is booted by Secure Zephyr
    - Normal calls services in secure via secure call
    - Secure interrupts priority > secure threads priority > normal interrupts priority > normal threads priority



ARM Trust-Zone M based



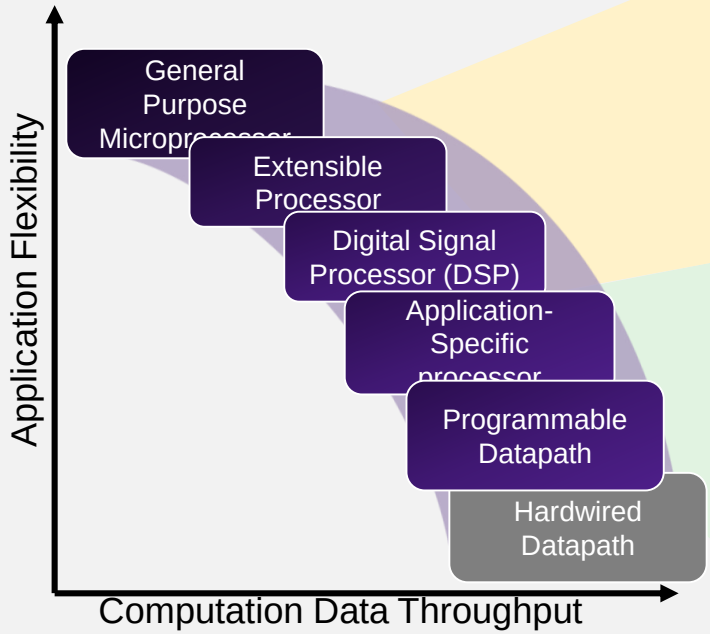
ARC SecureShield based

Zephyr in Synopsys

Designware ARC processor support

Synopsys Processor Solutions

IP & Tools Address Broadest Range of CPU & DSP Requirements



ARC® Processor IP

- Performance-Power-Area optimized for embedded applications
- Highly configurable and extensible architecture
- Based on common, code-compatible ISA
- Broad commercial and open source ecosystem

ASIP Designer Tool

- Automates creation of application-specific instruction-set processors (ASIPs)
- User-designed, programmable processors tailored to a specific application
- When processor IP cannot meet PPA requirements and fixed hardware is not flexible enough

DesignWare ARC Processor IP

Unrivaled Efficiency for Embedded Applications

EM Family

- Optimized for **ultra low power** IoT
- 3-stage pipeline w/ high efficiency DSP
- Power as low as 3uW/ MHz
- Area as small as 0.01mm^2 in 28HPM

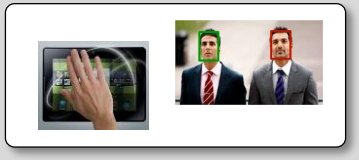
SEM Family

- **Security** processors for IoT and mobile
- Protection against HW, SW, and side channel attacks
- SecureShield enables Trusted Execution Environments

HS Family

- **Highest performance** ARC cores to date
- High speed 10- stage pipeline
- SMP Linux support
- Single, dual, quad core configurations

EV Family



- Heterogeneous multicore for **vision** processing
- State-of-the-art convolutional neural network (CNN)
- High productivity, standards-based tool suite

Already supported in Zephyr

ARC Support in Zephyr

ARC EM Starter Kit

- FPGA-based board
- 128 MB DDR3 RAM + PMOD interfaces
- Fmax 20-25 MHz
- Supports multiple EM processor configs

ARC IoT Development Kit

- ARC EM9D@55nm
- Arduino+ PMOD interfaces
- Fmax: 144 MHz
- 128 KB SRAM + 256 KB xCCM
- On board:
  - BLE
  - 9D Sensor

ARC EM Software Development Kit

- FPGA-based board
- 16 MB PSRAM + Arduino + PMOD + interfaces
- Fmax 50 MHz
- Supports all ARC EM Processors:
- On board
  - WiFi+BLE
  - 9D Sensor
  - Audio

ARC HS Development Kit

- 4 core ARC HS38
- 4 GB DDR3 RAM + Arduino + PMOD + interfaces
- Fmax 1 GHz
- On board
  - WiFi+BLE
  - HDMI
  - Ethernet
  - Audio

- ARC in Zephyr
  - <zephyr root>/arch/arc
- Supported features: User/kernel mode, MPU, Stack overflow check, DSP, fast IRQ, SecureShield(ARC EM), SMP (ARC HS)

Call to Action

- Want to learn more? Have some ideas? Get started here:
  - https://www.zephyrproject.org/
- Check out codebase on GitHub:
  - https://github.com/zephyrproject-rtos/zephyr
- Join our mailing list or hang out in our IRC channel
  - WeChat, QQ group
  - Slack(https://zephyrproject.slack.com)
- Join weekly on-line meetings, TSC meeting, secure, network, ….

SYNOPSYS®
Silicon to Software™

Thank You