SYNOPSYS®
Silicon to Software™

Zephyr: an Open Source RTOS for AIoT

Wayne Ren (任慰)

2019-08-24

Agenda

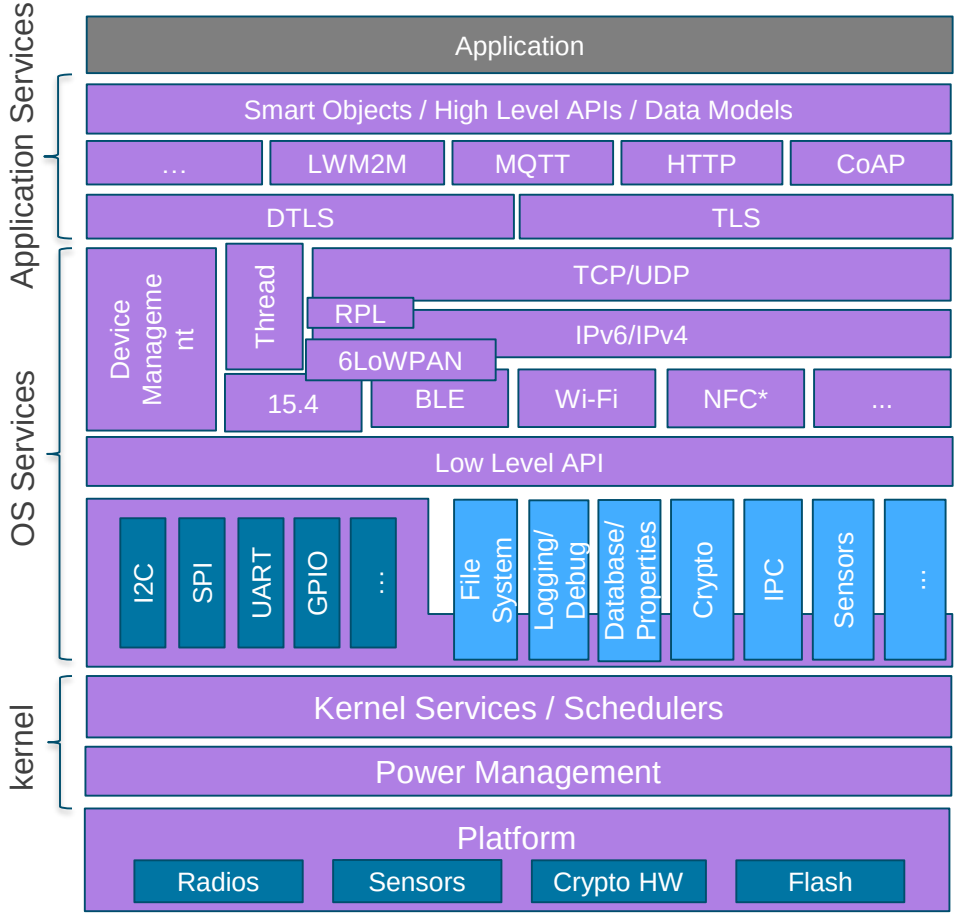
- Zephyr overview and status update
- Secure/safe design in Zephyr
- Synopsys Designware ARC processor support

Zephyr overview and status update

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 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 using LTS includes security updates
- **Certification** ready with Auditable

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

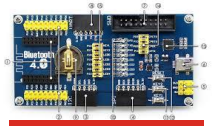
Zephyr Supported Hardware Architectures

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


SiFive HiFive1


Arduino Due


Nucleo 103RB


NRF51


Nucleo64


Nucleo F411RE


NRF52 pca10040


Nucleo F334R8


Synopsys


Arduino 101


Minnowboard


Altera MAX10


Nucleo 401RE


Hexiwear


ARM V2M MPS2


STM3210c


Atmel SAM E70


Adafruit Feather


Galileo


NXP FRDM


NRF52


Seeed Carbon


TI Launchpad

BBC Microbit


STM32373c


Redbear BLE Nano


96b Neon Key


Quark D2000


STM32 Olimexino


STM Mini A15


Seeed Nitrogen


ARM V2M Beetle


Zedboard


NXP FRDM-


tinyTILE


NXP i.MX RT1050

170 BOARDS TODAY WITH MORE ON WAY…

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

Zephyr’s Vibrant Community (2019/06/23)

Total Contributors

Rank	RTOS	#
1	mbed OS	532
2	**Zephyr**	**509**
3	nuttX	315

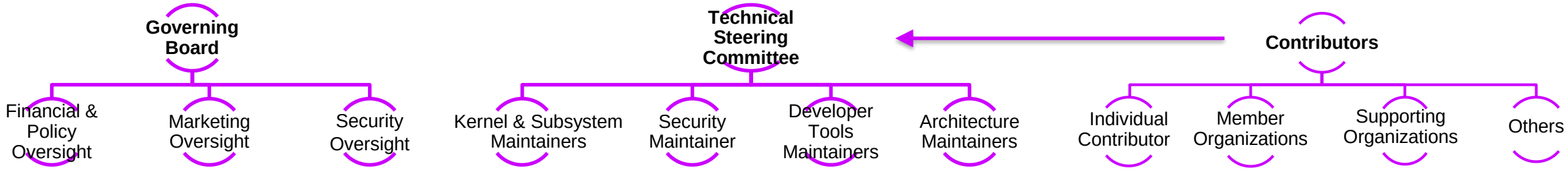
Total Commits

Rank	RTOS	#
1	nuttX	39,013
2	**Zephyr**	**32,206**
3	mbed OS	25,574

Commits to Master (last 30 days)

Rank	RTOS	#
1	**Zephyr**	900
2	mbed OS	269
3	RIOT	165

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

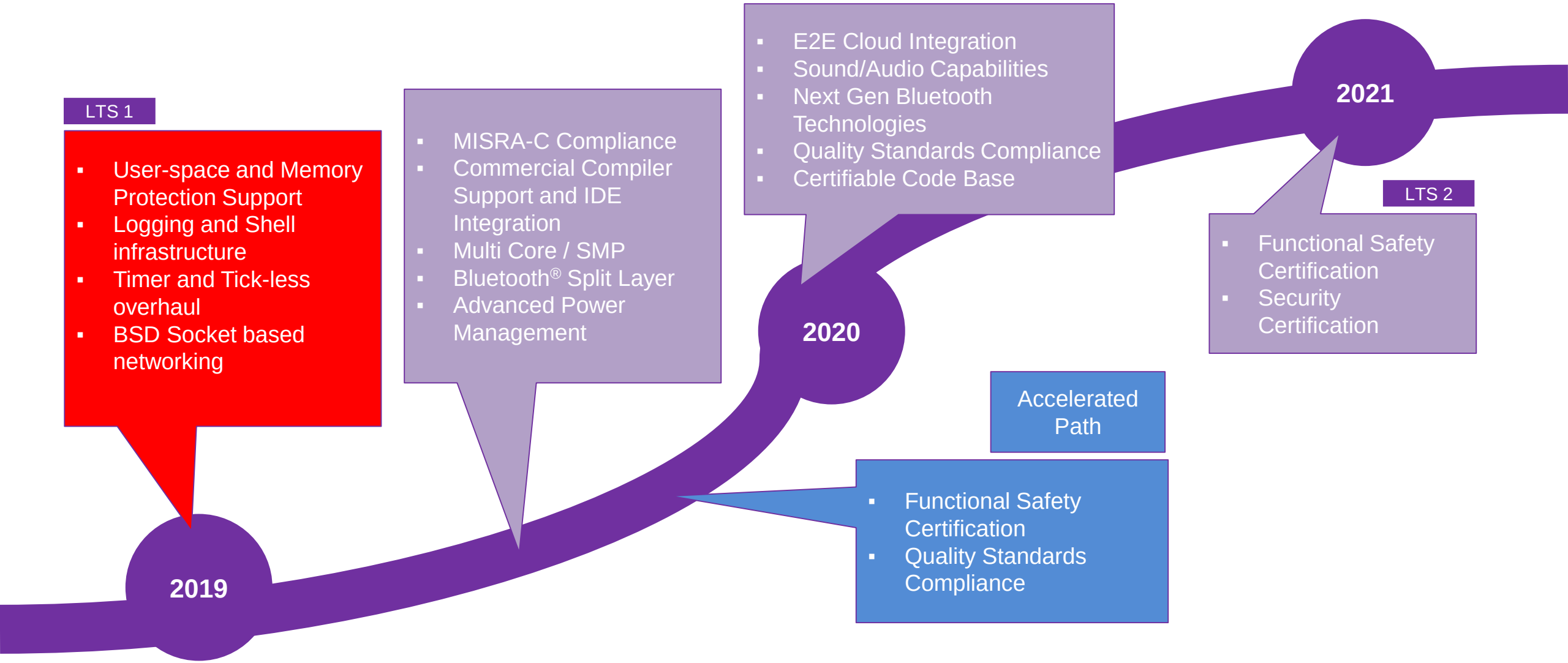
Community

- 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

- Zephyr 1.14 LTS (Long Term Support)
  - 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 ready
- Zephyr 2.0
  - RC1 is ready, formal release 2019.08.30
  - Outstanding features
    - ARC: multicore support and initial TEE support
    - ARM: Cortex-R support
    - 6LoCAN implementation
    - QEMU ARMv8-M

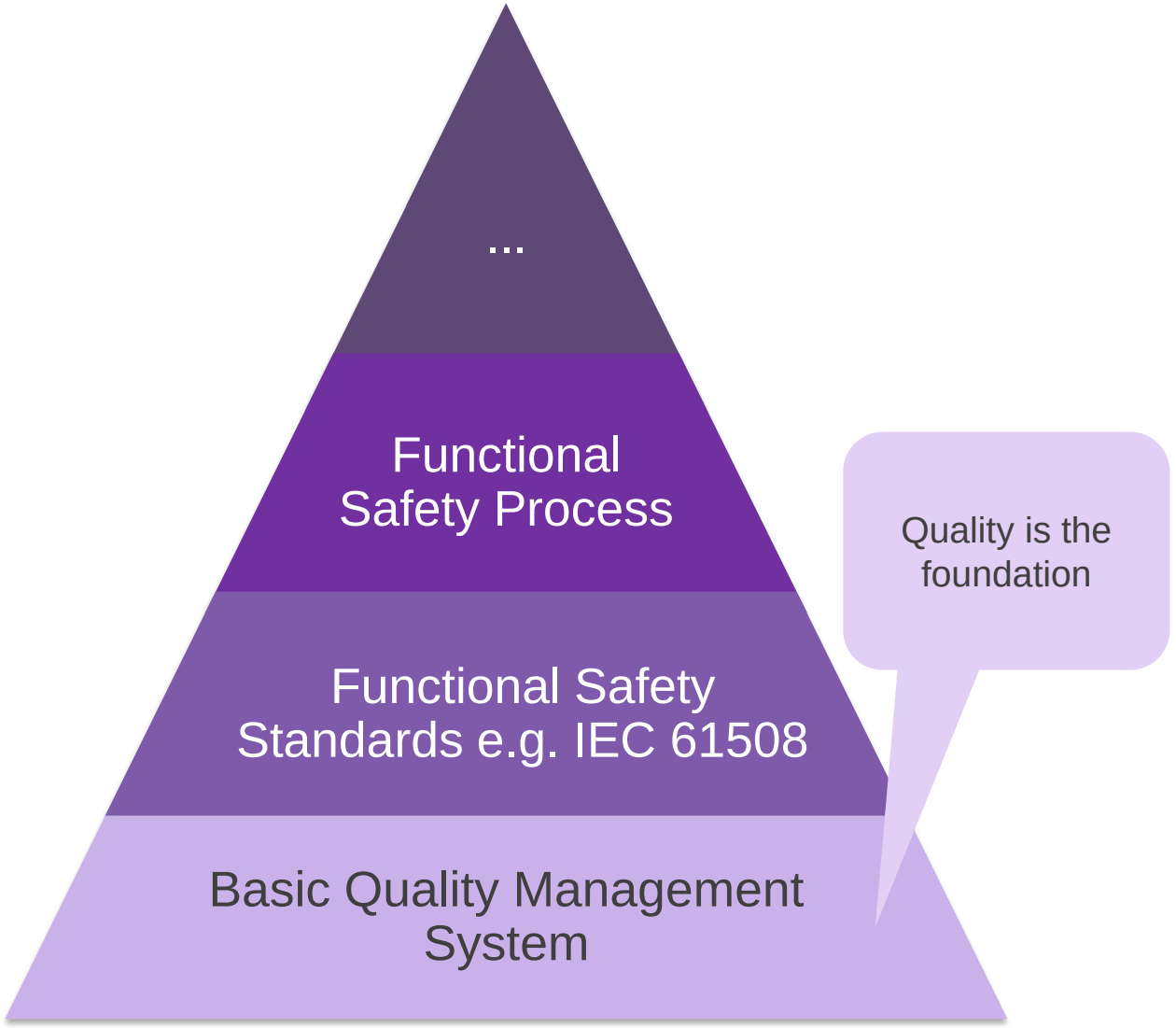
Zephyr Project Roadmap



Secure/safe design in Zephyr

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

- Contribute guidelines
- checkpatch

- Experienced reviewers
- > 2 reviewer approves

- Bug fixes
- Issues clean up
- Additional release tests
- Automatic regression tests

- Product ready

(Pre-certified)

- MISRA C
- FuSA
- CVE processing

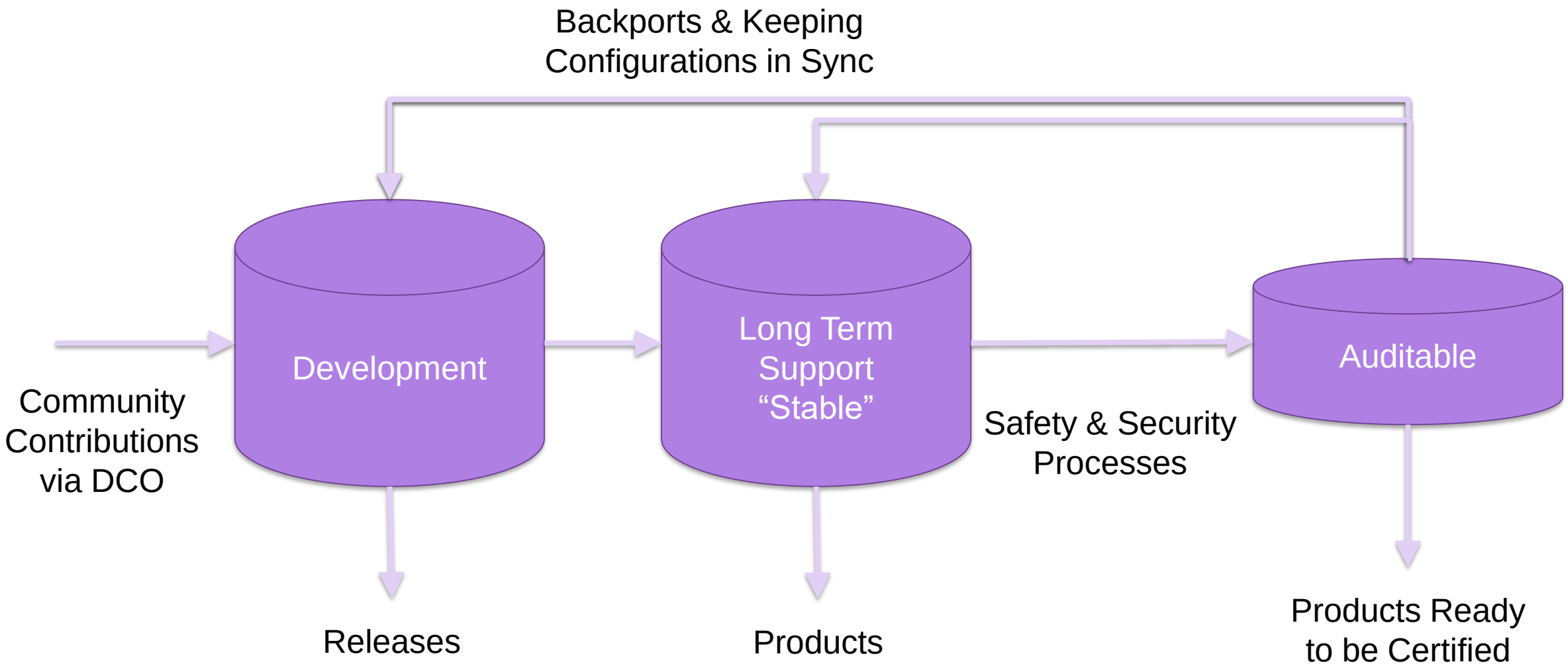
PR | CI | Review | Merge | Release | LTS | Auditable

- Shippable is used
- License
- Coding style
- Sanitycheck build
- Git commit format

- Daily run Test
- Coverity check
- Sanitycheck run

- Product ready
- Stable
- More tested

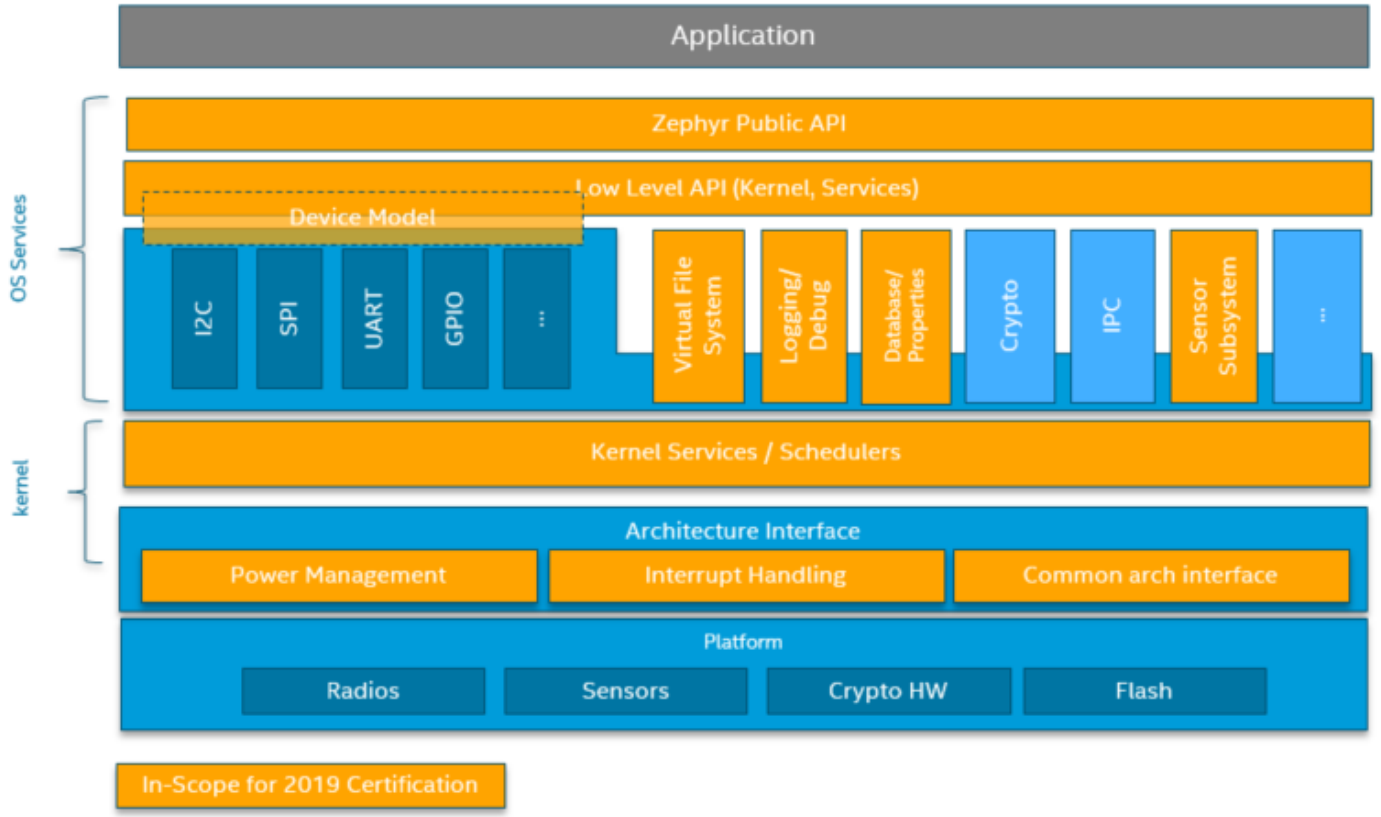
Code Repositories



2019 Auditable Scope (in orange)

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



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

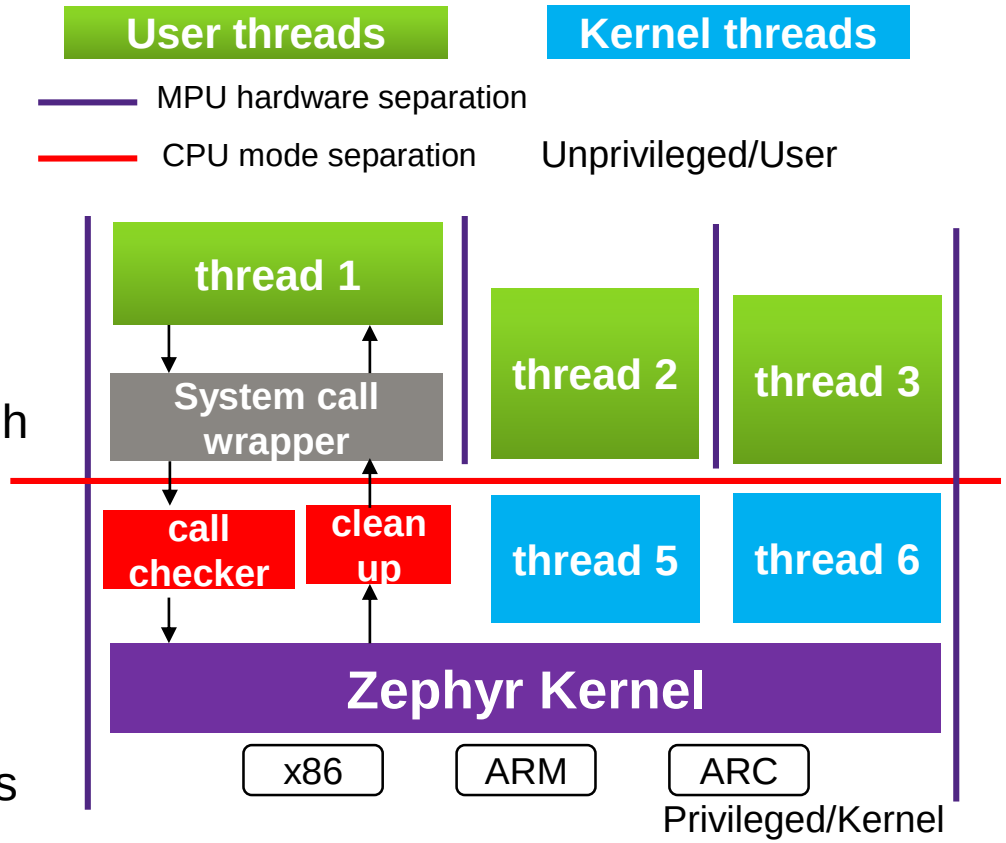
Zephyr OS: Auditable Considered Standards

- **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 (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
- **Security:**
  - PSA (Level 1+), Common Criteria (EAL4+), FIPS(140-2)
- **Others:**
  - Medical: FDA 510(K), ISO 14971, IEC 60601; Industrial: UL 1998, ??

User Space in Zephyr

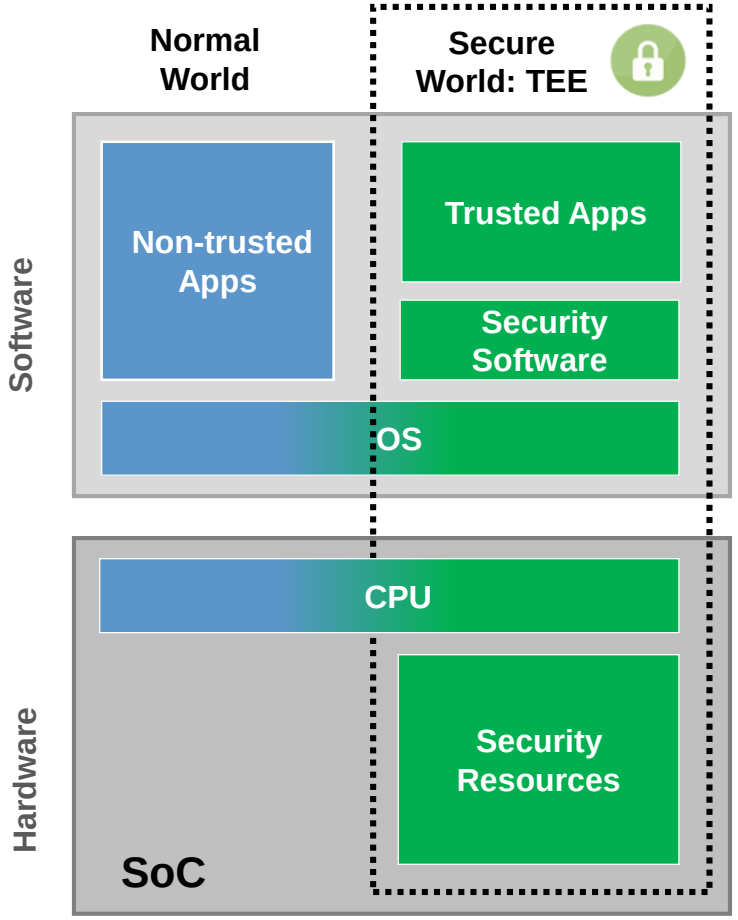
RTOS supporting user space are few

- 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



Trusted Execution Environment (TEE)

- Provides a secure area of the SoC to guarantee code and data protection
- Maintains confidentiality, integrity and authenticity of a system
- Code and data separation can be realized in software, hardware or a combination
  - Single CPU with HW separation
  - Physically separated secure CPU
  - Secure Module – companion to applications processor

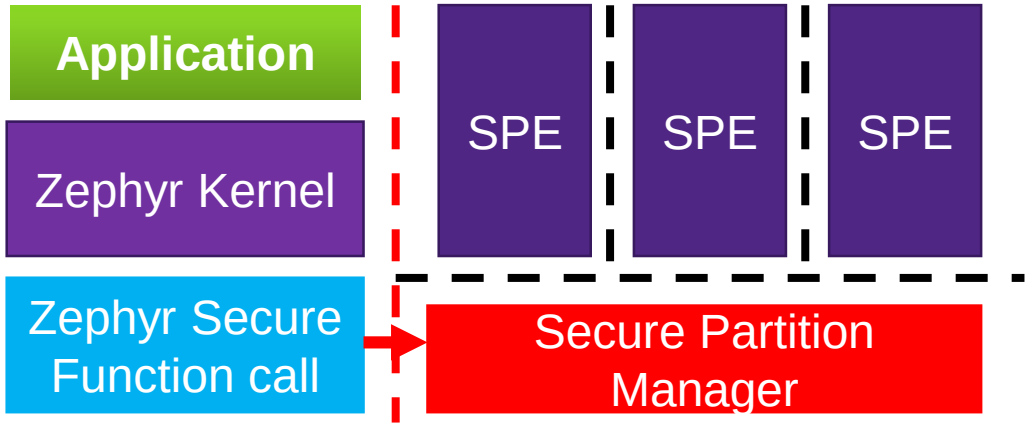


Example TEE implementation: Single CPU with HW Separation

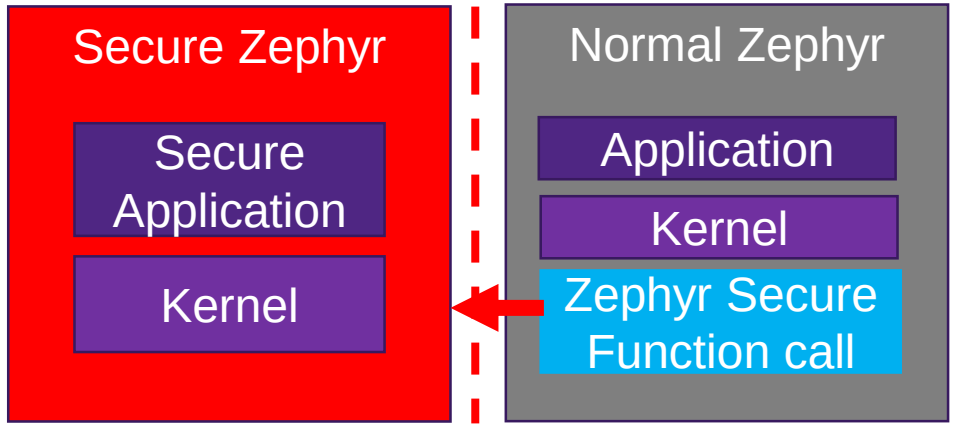
Zephyr and TEE

- 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

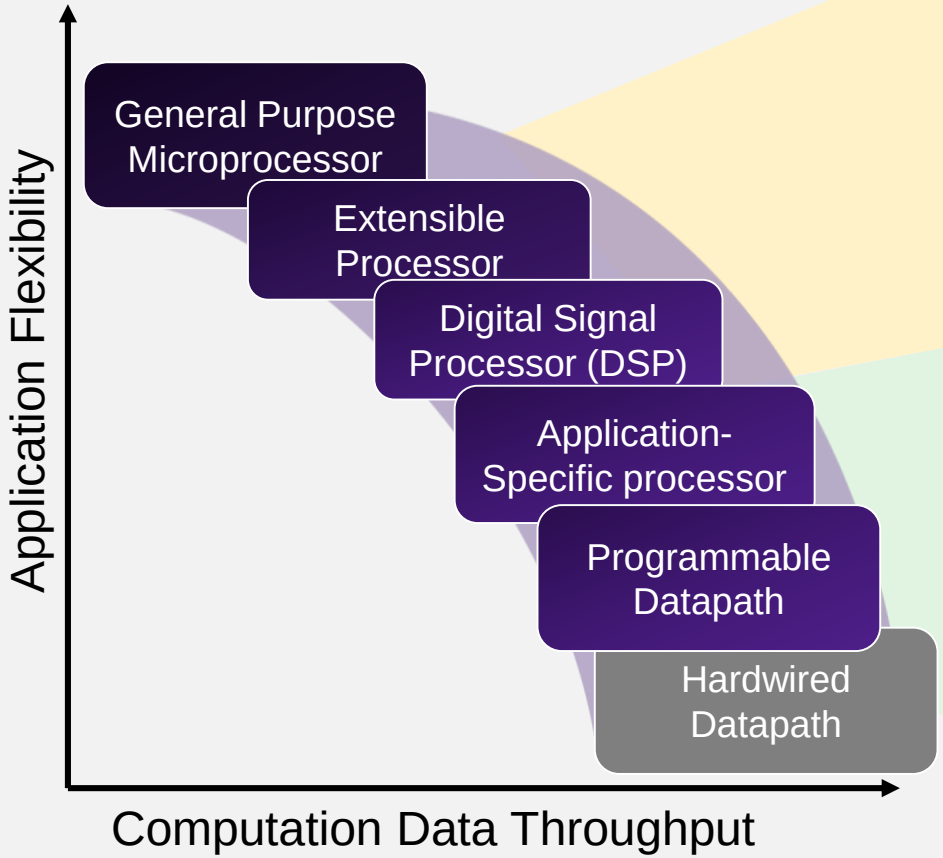


ARC SecureShield based

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

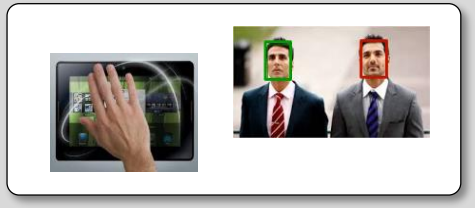
SEM Family

- **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 in Zephyr

Will be in Zephyr 2.0

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