

Zephyr Project Overview

A proven RTOS ecosystem, by developers, for developers



Use cases for a real-time OS







SMALL SCALABLE yet

< 8KB Flash

from small sensor nodes ... to complex multi-core systems





Heavily customizable

Out-of-the-box support for 450+ boards and 100s of sensors

Built with safety & security in mind Certification-ready Long-term Support







OPEN-SOURCE

Permissively licensed (Apache 2.0)

Vendor-neutral governance

ECOSYSTEM

Vibrant community

Supported by major silicon vendors

Features overview

- Comprehensive, lightweight, kernel & supporting services
 - \circ Fits where Linux is too big
- Inherently **portable** & **secure**

• Highly connected

- Bluetooth 5.0 & BLE
- Wi-Fi, Ethernet, CANbus, ...
- IoT protocols: CoAP, LwM2M, MQTT, OpenThread, ...
- USB & USB-C

• Developer-friendly

• Logging, tracing, debugging, built-in shell, Windows/Linux/macOS support, ...





Products Running Zephyr Today







Proglove

Ruuvi Tag



PHYTEC Distancer



Keeb.io BDN9



Hati-ACE

Oticon More



Adhoc Smart Waste



GNARBOX 2.0 SSD



Anicare Reindeer Tracker



Safety Pod



BLiXT solid state circuit breaker



Moto Watch 100



Lildog & Lilcat pet tracker



Rigado IoT Gateway



Livestock Tracker



Laird Connectivity sensors & gateways



BeST pump monitoring



Vestas Wind Turbines



zephyrproject.org/products-running-zephyr







Arduino Portenta H7

ESP32



Sipeed HiFive1



nRF9160 DK



STM32F746G Disco



M5StickC PLUS



TDK RoboKit 1



BBC micro:bit v2



Blue Wireless Swan



Arduino Nano 33 BLE



Intel UP Squared



Dragino LSN50 LoRA Sensor Node



Microchip SAM E54 Xplained Pro Evaluation Kit



Raspberry Pi Pico



Altera MAX10



NXP i.MX8MP EVK



Adafruit Feather M0 LoRa



u-blox EVK-NINA-B3





180+ Sensors Already Integrated

amg88xx







nrf5 nuvoton adc cmp npcx nxp_ki adec ma qdec_nrfx rpi_pico_temp

sm351lt th02 ti_hdc ti hdc20xx tmp108 tmp116 v15310x wsen_itds

Zephyr[®]

github.com/zephyrproject-rtos/zephyr/tree/main/drivers/sensor









Cortex-M, Cortex-R & Cortex-A



x86 & x86_64



docs.zephyrproject.org/latest/hardware/index.html#hardware-support

Vibrant Ecosystem





Development Tools





Applications & Middlewares



Training & Consulting



Firmwares & Libraries



Architecture



Application





Diving into Zephyr's features



IoT Connectivity Options



- Wide variety of **communication protocols**
 - Ethernet, 802.15.4, Thread, LoRa, Bluetooth, CAN bus, ...
- **Core network protocols** like IPv6, IPv4, UDP, TCP, ICMPv4, and ICMPv6.
- **Security** (ex. TLS, DTLS, ...)
- **Cloud integration** using MQTT, CoAP and HTTP protocols
- Over-the-air updates
- **Device management** using OMA LwM2M 1.1 protocol

Native IP Stack

- Built from scratch, on top of Zephyr native kernel concepts
- Dual mode **IPv4/IPv6 stack**
 - DHCP v4, IPv4 autoconf, IPv6 SLAAC, DNS, SNTP
- Multiple network interfaces support
- Time Sensitive Networking support
- BSD Sockets-based API
- Supports IP offloading
- Compliance and security tested





Bluetooth Host and Mesh



- Bluetooth 5.3 compliant
- Highly configurable
- Portable to all architectures supported by Zephyr
- Low Energy & experimental Bluetooth Classic
- IPSP/6LoWPAN for IPv6 connectivity over Bluetooth LE
- Multiple HCI transports

Bluetooth Low Energy Controller



- **Bluetooth 5.3 compliant** and qualified (5.1)
- Support for multiple BLE radio hardware architectures
 - Nordic nRF5x on Arm Cortex-M
 - VEGAboard on RISC-V
- Proprietary radios (downstream only)
- Unlimited role and connection count
- Concurrent multi-protocol support ready
- Multiple advertiser and scanner instances

Zephyr USB Device Stack



- USB 2.0 & USB-C support
- Supports multiple MCU families (STM32, Kinetis, nRF, SAM,...)
- Supports most common devices classes: CDC, Mass Storage, HID, Bluetooth HCI over USB, DFU, USB Audio, etc.
- Tight integration with the RTOS
- Native execution support for emulated development on Linux
- WebUSB support

Power Management



- Goal: use as little power as possible
- Cross-platform (architecture / SoC agnostic)
- Tickless scheduler
- Handled by the kernel / Customizable by the user

hardware on the target system **Decouple** the application from the hardware

docs.zephyrproject.org/latest/build/dts

Describe & **configure** the available

© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.

.dts file example

Devicetree

```
pinctrl-0 = <&i2c1_scl_pb8 &i2c1_sda_pb9>;
    pinctrl-names = "default";
    clock-frequency = <I2C_BITRATE_FAST>;
    status = "okay";
    lsm6ds1@6a {
        compatible = "st,lsm6dsl";
        reg = <0x06a >;
    };
    hts22105f {
        compatible = "st,hts221";
        reg = <0x5f >;
    };
    // ...
};
```

&i2c1 {



Secure boot / Device Management



- Leverage **MCUboot** as secure bootloader
- Application binary can be signed/encrypted
 Can use hardware keys
- But also:
 - Downgrade prevention
 - Dependency checks
 - Reset and failure recovery
- Over-the-air (OTA) upgrades
 - OMA LwM2M, Eclipse hawkBit
 - Vendor offerings

Hardware security



- Random Number Generation, ciphering, etc.
- Supported by crypto HW, or SW implementation (TinyCrypt)

• Trusted Firmware integration

- Firmware verification/encryption
- Device attestation
- Management of device secrets





Building on POSIX



- Zephyr apps can run as native Linux applications
 - Easier to debug/profile with native tools
 - Connect to real devices using TCP/IP, Bluetooth, CAN
 - Helps minimize hardware dependencies during the development phase
- Re-use existing code & libraries by accessing Zephyr services through POSIX API
 - Easier for non-embedded programmers
 - Implementation is optimized for constrained systems
 - Supported POSIX subsets: PSE51, PSE52, and BSD sockets

A real-time OS



Benchmark on Arm Cortex-M4F running at 120 MHz

Operation	Time
Thread create	2.5 µs
Thread start	3.6 µs
Thread suspend	3.3 µs
Thread resume	3.8 µs
Context switch (yield)	2.2 µs
Get semaphore	0.6 µs
Put semaphore	1.1 µs

Graphical User Interfaces



- Drivers available for various types of displays
 - LCD
 - OLED
 - Touch panel displays
 - E-ink
- LVGL integration
- Support for video capture and output



© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.

Inter-Process Communication

• Built-in kernel services (see table)

• IPC service

- 1-to-1 or 1-to-many communications
- No-copy API
- **zbus** (Zephyr Message Bus)
 - 1-to-1, 1-to-many, or many-to-many channel-based communications
 - Synchronous or asynchronous

Object	Bidirectional?	Data structure
FIFO	×	Queue
LIFO	×	Queue
Stack	×	Array
Message queue	×	Ring buffer
Mailbox	~	Queue
Pipe	×	Ring buffer

Data passing objects available in Zephyr kernel





A typical zbus application architecture

Tracing & Debugging

- Advanced **logging** framework
 - Multiple backends (UART, network, file system, ...)
 - Compile-time & runtime filtering

• **Tracing** framework

- Visualize the inner-working of the kernel and its various subsystems
- Object tracking (mutexes, timers, etc.)

	Timestate	Content	Dent		Detail 1			-										
	81.351 623	535 720008	· Ib Task	Teady	120000	10##2000014	d, runs aft	er 4.3334 m	(142 eyeles)									
544	81.355 926	534 T20006	O Task	81.0p														
\$35	01.355 957	031 🗾 T20006.	. > Task	Run	Pune 2	07 0 34 (0	eyeles)											
526	81.355 957	031 W T20006	- > Tesk	Run	Pune 1	or 4.4250 s	as (145 cycl	eo)										
247	01.335 957	The Troces			return	a after 11	.4921 88.											
249	41 141 177	734 1010		Enter .														
53.0	81,347 177	734	1 148	Esta:	Between	a to bile												
633	01.340 351	543 d Idle	O Task	81.00														
532	01.360 382	090 Z T20006.	> Task	Run														
533	01.347 156	993 🗾 Idle	💙 18B	Enter														
534	81.347 156	982Idle	💙 180	Enter														
\$35	01.347 156	902 Idle	A ISB	Exit	Beturn	s to Idle												
36	81.377 136	230 Idle	V 100	Ester														
97	82.277 136	In Idle	7 188	ESLOY .	Red over 1													
28	82.317 136	ATR Idle	1100	ER10	MPLUES	a ve idle												
12	41, 147 115	479 1416	100	Enter														
41	\$1.347 115	479 Idle	Ib Task	Beady	120400	18-8200001-	H. runs aft	er 20.5 up 1	1 cucles)									
ü	81.387 145	996 Idle	A ISB	Exit	Beturn	a to Idle												
	12000110E2000 12000116-E2000 12000210F2000 1200028-012000 1200028-012000 1200028-4E2000 Ide		00.0 ma				1	1	1	i.	_	ni ni har		1	1	i I	1	- 1
	20000044 2000108 2000108 2000108 200010 200010 200000 200000 200000 200000 200000 200000 200000 200000 200000 2000000						-	-						-	8.		_	
-	fype tittes	Information I	Aun Courte Fr	mainty La	at Rus Time	Mit Plan Time	Max Run Time	Tax Fun Time	Aut Time's	Minihan	Timers	Wax-Run Timera						
	22 BO 768	B 0430003238		4142	11100 Fill	0.0005 m	8.7830 m	85.2050 me	16.6001 ma 1.	175 6.65	08 mg 0.87%	23.5407	2.30%					
	CT 0.1 100	# 0x20000538	-	OH	6.0.00	0.0005 H	a.reso m	0.0 m	13.3944 mg 1.	10% 9.91	10 ma 0.00%	18.7983	0.00%					
	0 9-2 768	@ 0x29003858	28	614	1.1500 mi	0.0905 m	9.9487 m	106.1694	30.9750 ma 3.	10%	10 ma 0.00%	43,3654	4.34%					
			50	10 Hz 6	9.8852 mil	0.0905 m	518.9514	4753.143	967.8344	78% 0	10 ms 0.00%	1117.67	111.77%					
	0																	
	0																	
	0																	
	O (Vere started.																	



Zephyr 3.5 (Oct. 2023) – What's new?

- **Dynamic modules** (LLEXT)
- Picolibc as the new default C standard library
- Static Code Analysis using **CodeChecker**
- Native simulator
- Improved integration with **LVGL**
- ... and more, see <u>Release notes 3.5</u>.



LVGL





Safety & Security



Code Repositories







Long Term Support (Zephyr 2.7.x)

- Product Focused
- Current with latest **Security Updates**
- Compatible with new hardware
 Functional support for new hardware is regularly backported
- **Tested**: Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- <u>Supported for 2+ years</u>
- **1** Doesn't include cutting-edge functionality

Long Term Support (LTS - 1.14)



Zephyrproject-rtor O Code ① Issues 8 Rufusses Tags	/ Zepfyr	N Dar	C 2001	e () Issues	t 289 ∏ Pull requests 498 © Actions Projects 58 Ⅲ Whil ① Secu	sky 0 lat ins	
Costyrv1.140 - crist15 Unwite	Zephyr 1.14.0 ■ wilk vessed this on Apr 16-128 controls to matter since this vesses We are plassed this on Apr 16-128 controls to matter since this vesses We are plassed to announce the release include: • The Zephyr prepet new supports over 160 different board configurations sparring 8 architectures. All Architectures are reproceed themed and	Coce Insue	s / zephyr Okinesa - 310 . * 1 86 Philinguets 488 O Actions El Projects # 10040 C Security (a traig	M out release nos 0 v1.14.2 > €35ab3o imparo =	Zephyr LTS 1.14.2 (Mainternance Re reacher research to reacter since the release This is an LTS maintenance release with fixes. Security Vulnerability Related	Cede O Issues 3	(Zophyr Main) © Unwerh (Mil +) Y fan (Mil) 🔶 fanne (Mil Mil Ti Putregents (Mil C) Discessions © Actions 📑 Projects (Mil) Q Food antidese
	visitated using one of the namy simulation particines appointed by the project CIBMU, Renota, ARO Simulator, and the native POSK configure project CIBMU, Renota, ARO Simulator, and the native POSK configure at old one of the security diverse merointy discussible of the security diverse the bulk as by functional of the security diverse the bulk as by functional of the security diverse the bulk as by functions of the security diverse the bulk as by functions of the security diverse the bulk as by functions of the security diverse the other security diverse the security diverse the security diverse the security diverse set of com. The security cleanses the test security cleanses the secure code.	during one of the many simulation platforms supported by the BRUM, Revoor, ARC Simulanes, with a water MOSIX configura- ng subsystem has been revealed and simplementad, greatly in the matter during duriner, wenning thousands of lines Simplements during duriner, and escalation at all architectures. Simplements during duriner, and escalation at a statistications. Simplements during duriner, and escalational of lines were dusting of a were CPU atting AH that can right threads to cover has support the add, simplement cover, in robot most statistic for components at the cover of the second of the CRUM types, support architectures of the cover is in SMP mode by default, our first greatform to do non- umed the matery of components and protocols to use the curied the matery of components and protocols to use the curied by the cover of the during the during statistic during and one of the CRUM types. Lines on arking the optical to do non- mode the matery of components and protocols to use the curied the matery of components and protocols to use the curied the matery of components and protocols to use the curied the matery of the theorem types of the statistic during the statistic during statistic during statistic during the st		The relea	The following security vulnerabilities (CVEs) were addressed in this measure - CVE-0202-10019 - CVE-0202-10021 - CVE-0202-10022 - CVE-0202-10023	23 days ago nashif 0 v114.3 @ 0 r277365 Compare •	Zephyr v1.14.3 (International Content of Security Vulnerability Related
					CARE-020-10024 CARE-020-10027 CARE-020-10027 CARE-020-10028 More sealadi information can be found in: Https://docs.zephyproject.org/states/security/vulnerabilities.html Issues Fixed These GitHub issues were addressed since the previous 1.14.0 tagged release:		The totowing security vulnerabilities (CVEs) were addressed in this extension: • CVE-2020-10066 • CVE-2020-10069 • CVE-2020-10801 • C
			Qualification: 1.14.x Host subsystem qualified with QDD 139258 1.14.x Mesh subsystem qualified with QDD 139259 1.14.x Device component: qualified on Nordic nIMS2 with QDD 136679 Issues Fixed				These Ditkub issues were addressed since the previous 14.0 tagged release: + #8334 - DNS resolution is bream for some addresses in master[20-pre + #8097 - Burtocht, Controller: Mission (LL_BVC, 269 after HOLLIX:Negative Reply + 20109 - LL_BXEREM and Thereolene data bar entry in LL_DC and a tagged in the + 20109 - Instantenties, part land on miner(100, park bard). + 20109 - Instantenties, park land on miner(100, park bard).

Delivered bug fixes and latest security updates for 2 years!

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



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



Zephyr Security Overview introduction Current Security Definition Secure Development Process Secure Design Security Ventification Security Ventification

Security Vulnerability Reporting Secure Coding Sensor Device Threat Model Hardening Tool Vulnerabilities Samples and Demos

v: latest -

Zephyr Project

Docs / Latest » Security » Zephyr Security Overview O Open on GitHub

This is the documentation for the latest (main) development branch of Zephyr. If you are looking for the documentation of previous releases, use the drop-down menu on the left and select the desired version.

Zephyr Security Overview

Introduction

This document outlines the steps of the Zephyr Security Subcommittee towards a defined security process that helps developers build more secure software while addressing security compliance requirements. It presents the key ideas of the security process and outlines which documents need to be created. After the process is implemented and all supporting documents are created, this document is a top-level overview and entry point.

Overview and Scope

We begin with an overview of the Zephyr development process, which mainly focuses on security functionality.

In subsequent sections, the individual parts of the process are treated in detail. As depicted in Figure 1, these main steps are:

- Secure Development: Defines the system architecture and development process that ensures adherence to relevant coding principles and quality assurance procedures.
- 2. Secure Design: Defines security procedures and implement measures to enforce them. A security architecture of the system and relevant sub-modules is created, threats are identified, and countermeasures designed. Their correct implementation and the validity of the threat models are checked by code reviews. Finally, a process shall be defined for reporting, classifying, and mitigating security issues..
- Security Certification: Defines the certifiable part of the Zephyr RTOS. This includes an evaluation target, its assets, and how these assets are protected. Certification claims shall be determined and backed with appropriate evidence.



Software Supply Chain



- Zephyr ships an **SBOM** (Software Bill of Materials) with each release
- Downstream consumers can leverage built-in tools to, in turn, generate source & build SBOMs for their deliverables

```
[...]
FileName: ./zephyr/zephyr.elf
SPDXID: SPDXRef-File-zephyr.elf
FileChecksum: SHA1: e74cebcac51dabd799957ac51e4edcd32541103d
[...]
Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM SPDXRef-File-dev-handles.c
Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM SPDXRef-File-isr-tables.c
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libapp.a
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libzephyr.a
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libisr-tables.a
```

CVE Numbering Authority



<u>Registered with MITRE</u>

in 2017

- We issue our own CVEs
- Zephyr Project Security Incident Response Team (PSIRT)
 - Volunteers from the Security
 Subcommittee led by the Zephyr
 Security Architect.

Zephyr Project

The majority of the links on this page redirect to external websites E; these links will open a new window or tab depending on the web browser used.

Scope	Zephyr project components, and vulnerabilities that are not in another CNA's scope
Root	MITRE Corporation
Security Advisories	View Advisories
Program Role	CNA
Organization Type	Vendors and Projects
Country*	USA

OpenSSF Gold Badge

- <u>Core Infrastructure Initiative</u> Best Practices Program
- Awards badges based on "project commitment to security"
- Mostly about project infrastructure: is project hosting, etc following security practices
- Gold status since Feb, 2019



Zephyr Project

xpand 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 an Open Source Security Foundation (OpenSSF) best practices badge. Show details

If this is your project, please show your badge status on your project page! The badge status looks like this: openssf best practices gold Here is how to embed it: Show details

These are the passing level criteria. You can also view the silver or gold level criteria.

✓ Basics	13/13 •
✓ Change Control	9/9 •
✓ Reporting	8/8 •
✓ Quality	13/13 •
✓ Security	16/16 •
✓ Analysis	8/8 •



Vulnerability Alert Registry



- For an embargo to be effective, product makers need to be notified early so they can remediate
- <u>Goal</u>: 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



Zephyr PSIRT: Remediation and Response

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, <u>CVE-2020-17468</u>, and <u>CVE-2020-17469</u>, are in the IPv6 Fnet code, one, <u>CVE-2020-17467</u>, affects Link-local Multicast Name Resolution LLMNR), and 2, <u>CVE-2020-24383</u>, and <u>CVE-2020-17470</u> 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.



Forescord Research Labe has launched Preject Memoria, an historie that aims at providing the community with the largest study on the security of TCP/PF stacks. Project Memoria's goal is to develop the understanding of common bugs behind the valuerabilities in TCP/P stacks, identifying the threats they pose to the extended enterprise and how to milgate those.

<) FORESCOUT

 AMMESIA-33 is the first study we have published under Project Memoria. In this study, we discuss the results of the security analysis of seven open source TOP/IP studs and report a bundle of 33 new viewebilities found in four of the seven analyzed stacks that are used by major lof, OT and IT device vendors.

• Four of the vulnerabilities in ANNISIA-33 are entited, with potential for enrote code neuroism on entral molecular Supporting Theorem Anneabilities could allow an attacker to take control of a device, thau using it as an entry point on a network for intermet-content devices, as a joint point for lateral movement, as a persistence point on the target network or an the final target on attack. For entremet-content devices, as a joint point and the final target of an attack. For entremeting comparison, this means they are al increased risk of having their network comporting of a having maincious actions undermine their business contribuly. For comments, this means that their to Tedeose may be used as part of large attack comparison, such to bortest, without them being avec.

forescout.com/amnesia33/ research@forescout.com tol fee 1-866-377-877



AMNESIA:33 | EXECUTIVE SUMMARY

Zephyr Security Summary









Documented secure coding practices

Vulnerability response criteria publicly documented Weekly Coverity scans MISRA scans SBOM generation



Certification



Initial certification focus



- Start with a limited scope of kernel and interfaces
- Initial target is IEC 61508 SIL 3 / SC 3 (IEC 61508-3, 7.4.2.12, Route 3s)
- x86 and ARM is initial focus
- Scope will be extended to include additional components as determined by the safety committee

		r RTOS	Zep		
Device Model / Devic Driver Model	nel and services	w Level API for		Public Kernel API	Zephyr
OS Services				s, and Synchronization	nel Services
File System API	dition Variables	Semaphores	Interrupts	Scheduling	Threads
Logging / Debug	Symmetric	utexes / Fulex	olling API (Event	Workqueue	System Threads
Settings (Database / properties)	unprocessing		Pointy		Jata passing
Architecture Interfac	i	0	fessage Queues	LIFQs	Queues
Power Managment		Pipes	Malboxes	Stacks	FIFOs
Interrupt Handling		er services)	Miscellanous (C	Memory Managemen	Iming
Common Architecture Interfaces	Fatal errors	Floating po services	CPU idling	Memory Heaps	Kernel Timing
MMU7MPU	Thread local storages	Version	Atomic servicces	Memory Slaps	Timers

Safety Collateral Proposal



Draft	(pending approval by Certification Authority)				
Phase	Assumed Collateral	Type of Doc	Owner	Sharing Model	
	Safety Plan and Safety Assessment Plan	Plan/Process	FSM	Platinum	٠
	Verification / Validation / Integration Test Plans	Plan/Process	Testing WG	Public	
pt	Software Development Plan	Plan/Process	TSC	Public	-
UC	Configuration and Change Management Plans	Plan/Process	TSC	Public	-
ပိ	Software Architecture and Module Design Specification	Plan/Process	TSC	Public	+
fety	Coding Guideline	Plan/Process	TSC	Public	*
Saf	Tools Documentation	Plan/Process	TSC	Public	+
	Software Requirements	Code	TSC	Public	+
	Software Safety Requirements Specification	Result Artifact	Safety WG	Platinum	+
	Tests (Integration, Arch / Module, Validation)	Code	TSC	Public	
	Code Review Report	Result Artifact	Safety WG	Platinum	-
	Verification / Validation / Integration Test Reports	Result Artifact	Testing WG	Platinum	+
e	Fault Injection Test Report	Result Artifact	Testing WG	Platinum	+
has	Tools Classification	Result Artifact	Safety WG	Platinum	*
st P	Tools Validation	Result Artifact	Safety WG	Platinum	*
Tex	Traceability Report	Result Artifact	Testing WG/FSM	Platinum	-
led	Test Coverage Report	Result Artifact	Testing WG/FSM	Platinum	+
etai	Coding Guideline Compliance Report	Result Artifact	Safety WG	Platinum	-
ă	Safety Analysis (e.g., FMEA)	Result Artifact	FSM	Platinum	-
	Source Code	Code	TSC	Public	*
	Software User Manual	Result Artifact	TSC	Platinum	+
	Safety Manual	Result Artifact	FSM	Platinum	*
Silver r	nembers have limited access, restricted use to Platin	um artifacts ba	sed on participat	ion	

Compliant Development: V-model



- It is difficult to map a stereotypical open-source development to the V-model Zephyr RTOS functional safety work products mapping to IEC 61508-3 V model
- $\circ~$ Specification of features
- Comprehensive documentation
- Traceability from requirements to source code
- Number of committers and information known about them

⇒ Provide the evidences that open source developers can map to compliance and meet all requirements





Ecosystem & Governance













intel

🔿 Meta











Zephyr Project: Silver Members





Vibrant Ecosystem





Development Tools





Applications & Middlewares



Training & Consulting



Firmwares & Libraries

© 2023 The Zephyr Project — Content made available under CC BY-SA 4.0.

🛑 eclipse 🚊 🔛 Compilers **Debuggers / Tracing Tools** LAUTERBACH **Emulation / Simulation** RENODE WOKWI

Ecosystem // **Dev Tools**



IDE









@



6

Ecosystem // Training & Consulting





Training & Consulting



Firmwares & Libraries

Zephyr

Applications & Middlewares

Ecosystem // Firmwares & Libraries

EDGE IMPULSE

Ecosystem // Apps & Middlewares

Zephyr in the RTOS landscape

_

GitHub Stars History

 $2023-10-01 \rightarrow 2023-10-14$

~883 unique clones per day ~1212 unique visitors per day

Zephyr

github.com/zephyrproject-rtos

chat.zephyrproject.org

zephyrproject.org

