Open Source 西门子

Beijing · 2026

Oct. 29
Industrial Open Source

Oct. 30
Open Source Robotics

Agenda

面向功能安全的开源软件

Open Source Software for Safety-Critical Systems

王琪

WANG Qi

Unrestricted | © Siemens 2026 | Foundational Technologies | 2026-10-30

SIEMENS

About me



王琪
WANG Qi

西门子中国研究院
Foundational Technologies, Siemens Ltd., China

高级专家研究员
Senior Key Expert

认证功能安全工程师
Certified Functional Safety Engineer

研究方向：软件定义自动化
Research Topics: Software-Defined Automation

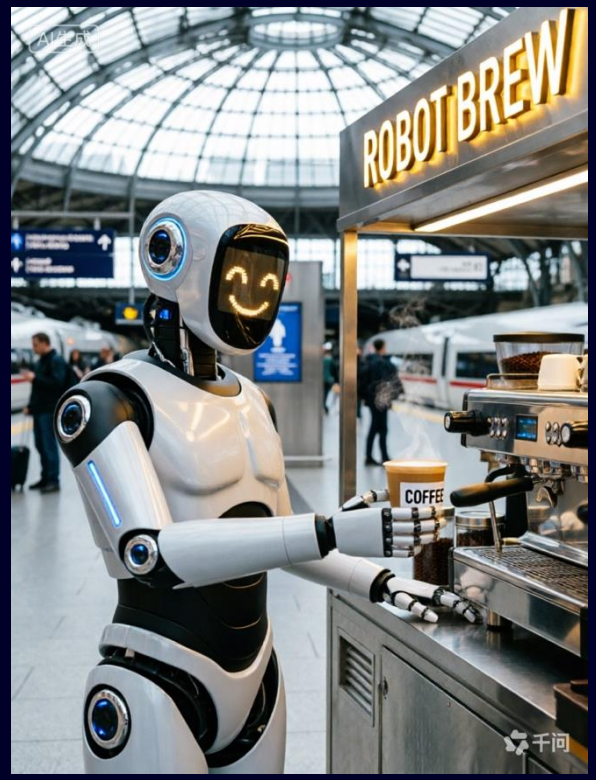
SIEMENS

Increasing Needs for Functional Safety of Humanoid Robots

Robots in Factory



Robots in Public



Robots at Home



Increasing needs for functional safety

SIEMENS

Safety Standards Relevant to Humanoid Robotics

ISO 21448:
Road vehicles - Safety of the intended functionality (SOTIF)

ISO 25785-1 (under development):
Robotics - Safety requirements for dynamically stable industrial mobile robots (legged, wheeled, or other forms of locomotion)

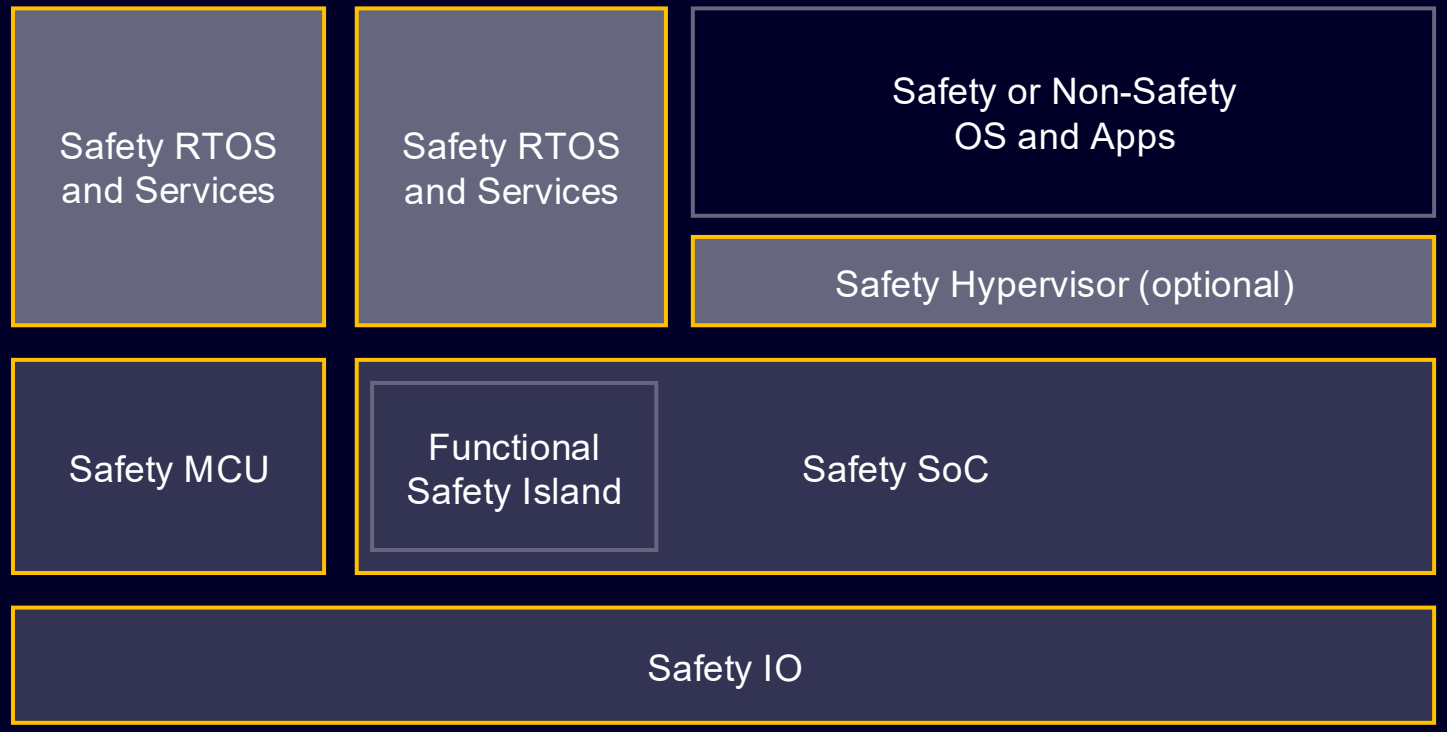
ISO 10218:
Robotics - Safety requirements for industrial robots

ISO 13849:
Safety of machinery - Safety-related parts of control systems

IEC 61508:
Functional safety of electrical / electronic / programmable electronic safety-related systems

SIEMENS

Mixed-Criticality Systems for Autonomous Driving and Robotics



Unrestricted | © Siemens 2026 | Foundational Technologies | 2026-10-30
SIEMENS

Safety is Expensive!

Apex.OS Cert with 24 ROS2 + native packages certified to ISO26262 (ASIL-D).

~ 65K
lines of code

14 person years
of effort

> 5 Million USD
cost in tool licenses, infrastructure and engineering resources

~ 3000 tests
newly added

100% coverage
on statement, branch and MC/DC

~ 300 safety requirements
generated from FMEA, TSC and Tools C&Q

~ 100 artifacts
(~2000 A4 pages) submitted

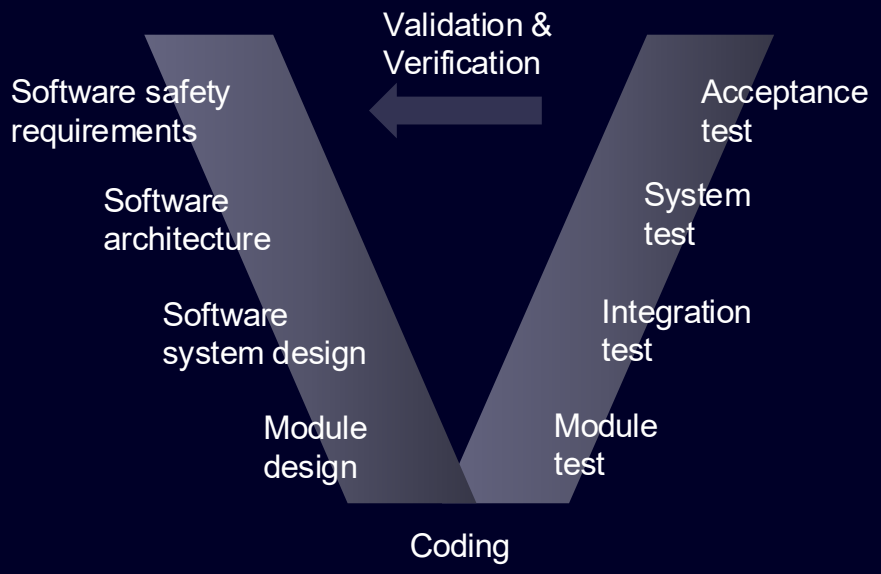
5 iterations
of audit conducted by TÜV NORD

Note: Numbers from Apex.AI presentation “Safe and certified software for autonomous mobility” in Embedded World 2021 (March 1-5).

SIEMENS

The Conflicts between Safety and Open Source Software

Safety Software Development
The V-Model



Open Source Software
Development Model



Verifiable & Evidence traceability

V.S.

Openness & Rapid iteration

SIEMENS

Open Source Projects for Safety

Supporting tools for safety certification	Safety certifiable open source	Safety certifiable + dev. model compliance	Safety supported by formal verification
ELISA for Linux	**ThreadX** RTOS	**Zephyr** RTOS	**seL4** Microkernel
ROS 2 Safety (inactive)	**Ferrocene** Rust Compiler	**Xen** Hypervisor	
	L4Re Microkernel		

SIEMENS

Zephyr RTOS Safety Activities



Project start

2016

Safety Committee established

2019

Concept approval for IEC 61508 certification of the Zephyr kernel

2024

Process formalization community contribution processes were still being defined across the V-model lifecycle

2025

Certifiable Completion of the Zephyr project certification

2027 or later

Certification Phase 1

- Approval of the overall plans and strategy, scope and high level requirements & architecture

Certification Phase 2 (gaps to be filled)

- Completeness of specifications, e.g., requirements, architecture
- Safety analysis, e.g., FMEA
- Traceability
- Verification & test coverage

Other achievements

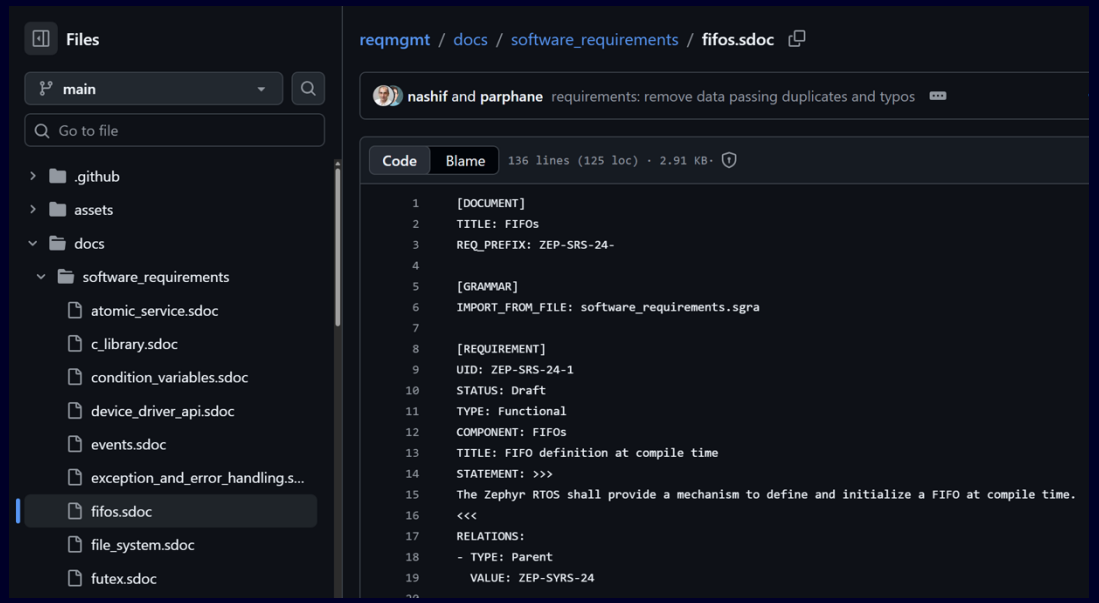
- Coding guidelines and static analysis tooling
- Automatic documentation of requirements from StrictDoc rules
- Requirements process was officially available, and reference requirements and traceability started in the code base

Reference: Zephyr: Learnings from Working on Safety Certification in the Open, OSS Japan, 2025

SIEMENS

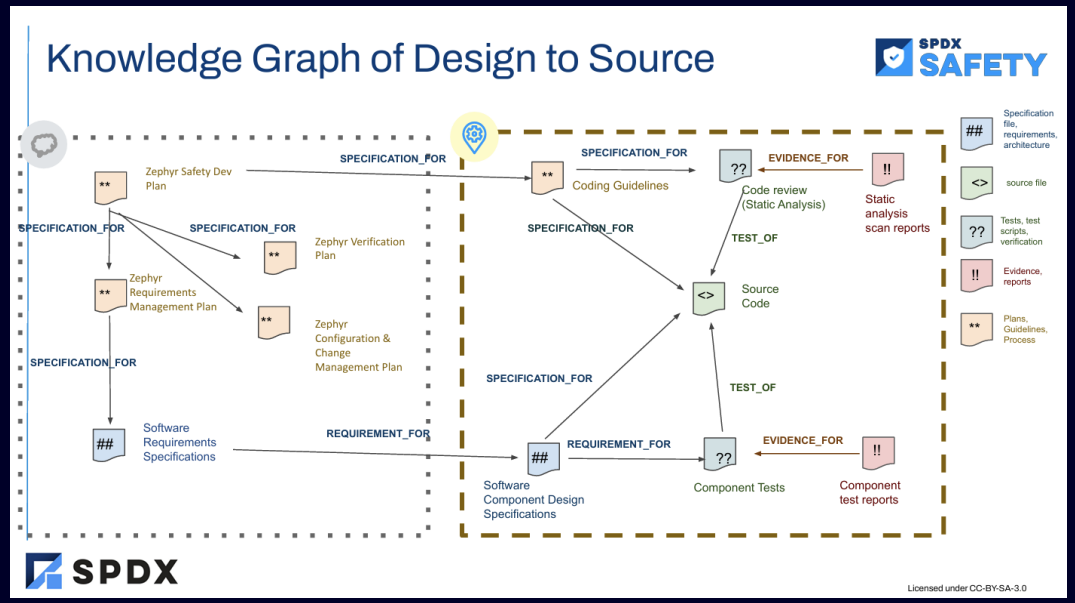
Open Source Tools for Documentation and Traceability

StrictDoc



StrictDoc is used for safety requirement documentation in Zephyr.

SPDX Safety Profile



SPDX for exchange safety information across software packages.

Reference: Zephyr: Learnings from Working on Safety Certification in the Open, OSS Japan, 2025

SIEMENS

seL4 Microkernel based on Formal Verification

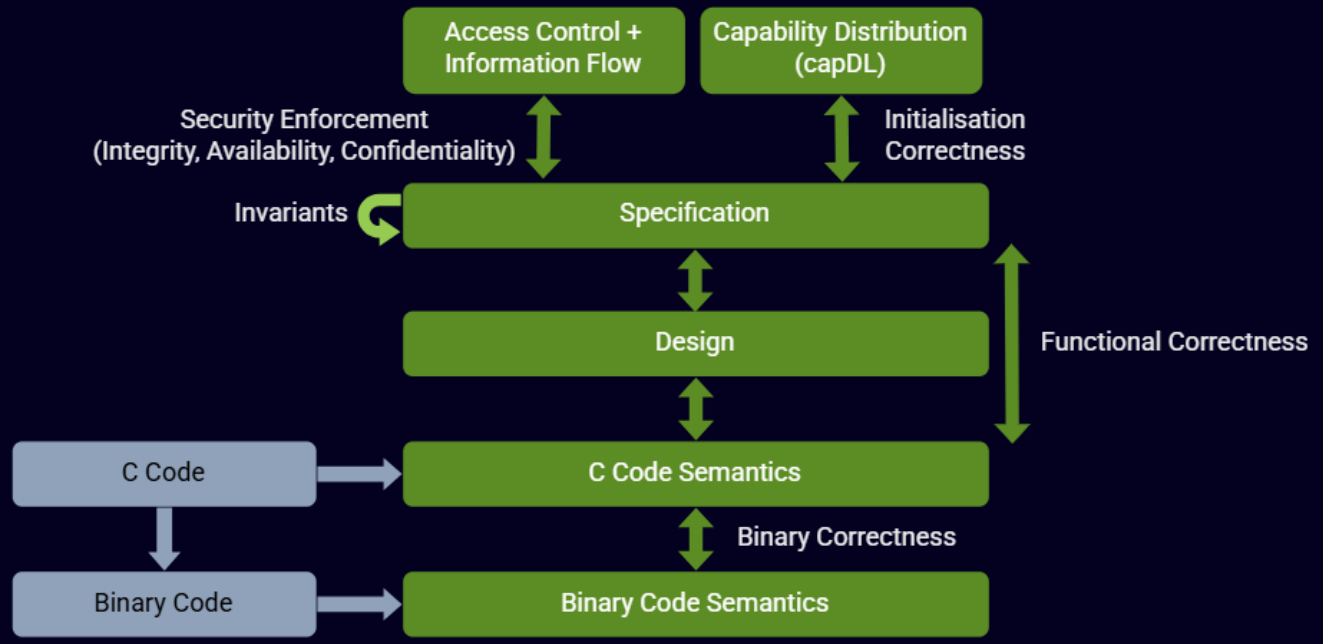
The world's first formally verified kernel.

"With its mathematical, machine-checked proofs of correctness and security, seL4's assurance level is considerably stronger than ISO26262 highest risk recommendations."

The seL4 proofs:

- C code functional correctness
- Binary correctness
- Security
- System initialization

The trend: AI for formal verification



SIEMENS

Summary

- Functional safety is mandatory for robots to collaborate with people.
- Open source for safety matters.
- Good progress achieved by open source software (e.g., Zephyr) for safety, but gaps still exist for being certifiable.
- A different approach for open source for safety is showed by seL4 based on formal verification.
- AI can be helpful.

SIEMENS

Thank you

WANG Qi
Senior Key Expert
Foundational Technologies
Siemens Ltd., China
wq.wang@siemens.com

Unrestricted | © Siemens 2026 | Foundational Technologies | 2026-10-30

SIEMENS

Open Source 西门子

Beijing · 2026

Oct. 29
Industrial Open Source

Oct. 30
Open Source Robotics

Agenda