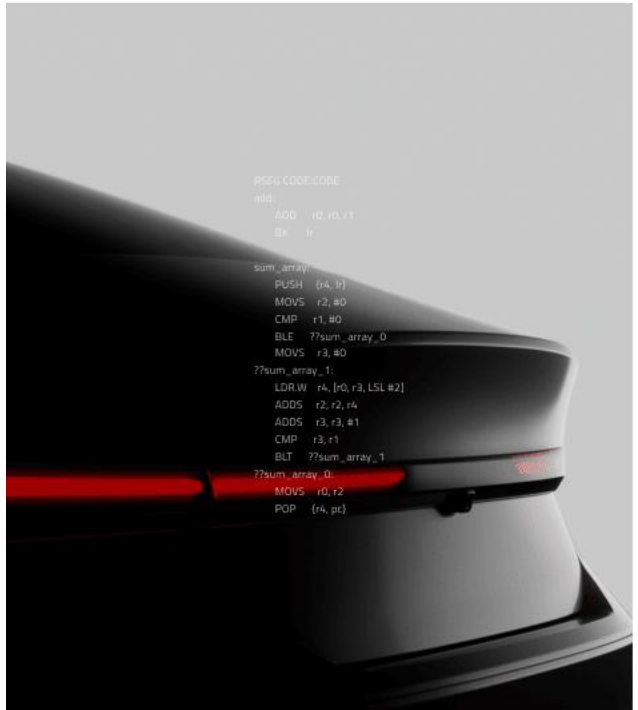
Powered by
Qt Group

IAR Platform加速机器人功能安全应用开发

潘锋
FAE
2026-10-12





机器人的安全成本，不是一次性认证，而是架构与标准两条轴上的持续成本

01 机器人功能安全的核心挑战
02 软件工具链的四项要求
03 IAR Platform 简介
04 总结

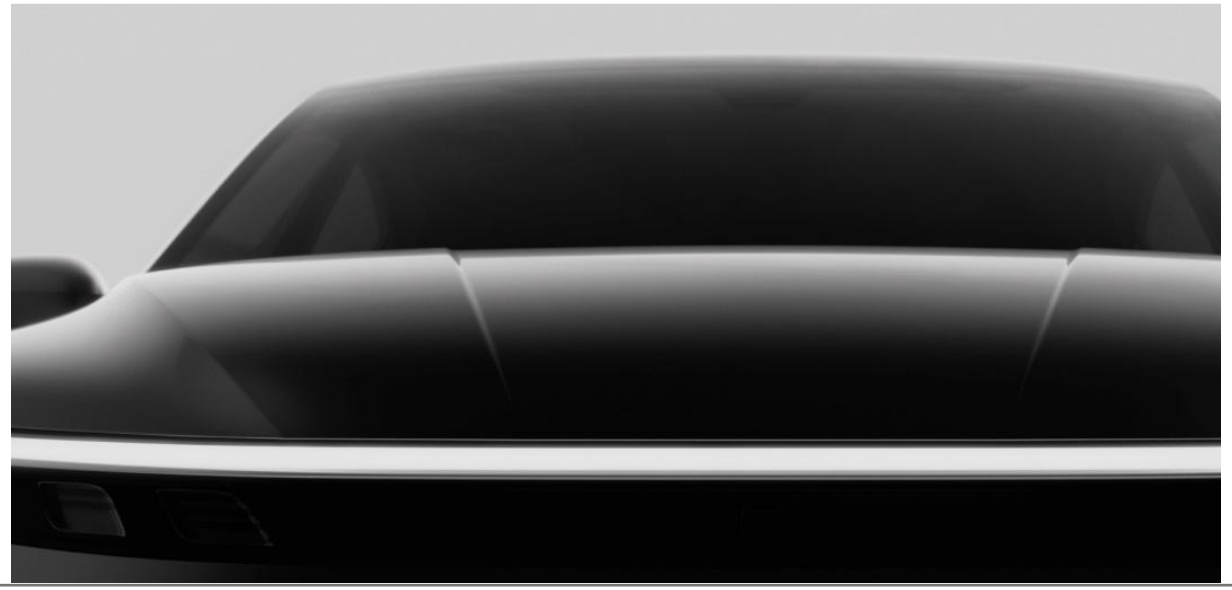
Copyright © 2026 Qt Group and its group companies. All rights reserved.

01

机器人功能安全的核心挑战

功能安全涉及风险评估、架构设计、认证流程与供应链等多个环节。本节仅就其中的软件开发工具链展开。





Copyright © 2026 Qt Group and its group companies. All rights reserved.

范围界定：安全关键功能的运行边界

确定性域：安全关键控制

- 伺服控制环路
- 力矩与力限制（PFL）
- 急停与安全联锁
- 编码器闭环与位置监控
- 安全限速与安全停止

行为可穷举、时序可预测，运行于实时 MCU / MPU，裸机或 RTOS。

对应标准：整机侧 ISO 13849-1；PFL 见 ISO 10218-2 与 ISO/TS 15066；驱动器侧 IEC 61800-5-2 安全子功能（STO / SS1 / SS2 / SOS / SLS / SBC）。

非确定性域：AI 与自主决策

- AI 视觉感知与 SLAM
- 路径规划与策略模型
- Linux 与 ROS 2 应用栈

输出为概率性，无法用同一套确定性论证覆盖，本次不展开。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

参考架构：整机安全职责的分层

① AI 决策层（Non-Trusted）　|　定级：QM，不做安全声明
大模型任务理解与语义规划；其失效由下层独立监控兜底
约束手段：输出格式强约束 · 越界检测 · 工具白名单（工程措施，不计入安全论证）

② 安全监控层　|　定级：PL d / SIL 2 起，关键功能 PL e / SIL 3
独立安全 MCU：独立供电、时钟、看门狗与传感器输入，与 AI 主控解耦
运动空间与速度限制（ISO 10218-2 · ISO/TS 15066 PFL）· 独立急停通道（ISO 13850）

③ 执行安全层（Trusted）　|　定级：PL d~e / SIL 2~3
伺服 · 关节电机 · 制动器 · 编码器
STO / SS1 / SLS / SBC 安全子功能（IEC 61800-5-2）· STO 仅去除转矩，承重轴需 SBC 抱闸兜底

AI 层不做安全声明，安全由监控层与执行层独立承担

Copyright © 2026 Qt Group and its group companies. All rights reserved.

挑战一：架构碎片化导致工具链碎片化

Arm

Cortex-M / Cortex-R

RISC-V

新一代开放架构

专有架构

RH850、AURIX、C2000、RX、RL78 .....

每换一种架构，编译、静态分析、调试与认证证据都要重建一遍

Copyright © 2026 Qt Group and its group companies. All rights reserved.

挑战二：机器人标准碎片化

汽车行业：单一中心

- ISO 26262 事实上统一全行业
- ASIL 分级与证据格式一致
- 供应链上下游共享同一套语言

一次投入，长期沿用同一套安全论证框架。

机器人行业：多标准并列

- ISO 10218-1 / -2：工业机器人（C 类）
- ISO/TS 15066：协作应用功率与力限制（PFL）
- ISO 13482：个人护理机器人，人形形态最接近
- ISO 3691-4：无人驾驶工业车辆（AGV / AMR）
- ISO 10218-2 明文把「机械臂 + 移动平台」排除在范围外。
- TS 15066 主体已并入 10218-2，其本身仍现行待修订；13482 第 2 版已至 FDIS。
- 多部 C 类标准按形态切分，无一覆盖人形整机；但对工具的要求指向同一处。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

标准引用链：从行业标准到根标准

① 应用型标准

ISO 10218-1

规定安全功能与所需 PL，不含软件与工具条款；规范性引用指向 ISO 13849-1

② 方法论层

ISO 13849-1

软件安全要求集中在 Clause 7；规范性引用 IEC 61508-3 与 IEC 62061

③ 共同落点

IEC 61508-3

§7.4.4 支持工具 T1 / T2 / T3 分类与已知缺陷清单 —— 工具要求的唯一出处

顶层标准不同，安全论证的路径相同

Copyright © 2026 Qt Group and its group companies. All rights reserved.

零部件路线：驱动器的标准链更短、工具要求更明确

① 子系统产品标准

IEC 61800-5-2

PDS(SR) 安全相关电气传动系统；SIL 上限 SIL 3

② 直接引用

IEC 61508

硬件与软件要求整体引用，不经由 ISO 13849

③ 工具条款

IEC 61508-3 §7.4.4

支持工具 T1 / T2 / T3 分类与已知缺陷清单

同一个落点，但驱动器这条路对工具的要求写得更明确

Copyright © 2026 Qt Group and its group companies. All rights reserved.

挑战三：长生命周期支持缺口

产品周期：以十年计

- 现场服役周期常达十年以上
- 持续固件迭代与安全补丁
- 安全论证需全周期有效
- 换料与停产迫使证据重建

十年后仍需复原当年的构建环境与证据。

工具支持周期：以年计

- 开源工具链版本更迭快，旧分支少人维护
- 缺少长期支持承诺与缺陷通告
- 历史构建环境难以完整复原
- 工具资质证据需自行准备与维护
- 迭代后需回归验证，原有保护是否仍成立

需要可长期锁定、且有责任方维护的工具版本。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

挑战四：标准未定型与先行出货的矛盾

现实处境

- 具身与移动机器人已在部署
- 专用安全标准尚未生效
- 只能用现有标准尽力覆盖
- 返工风险由厂商承担

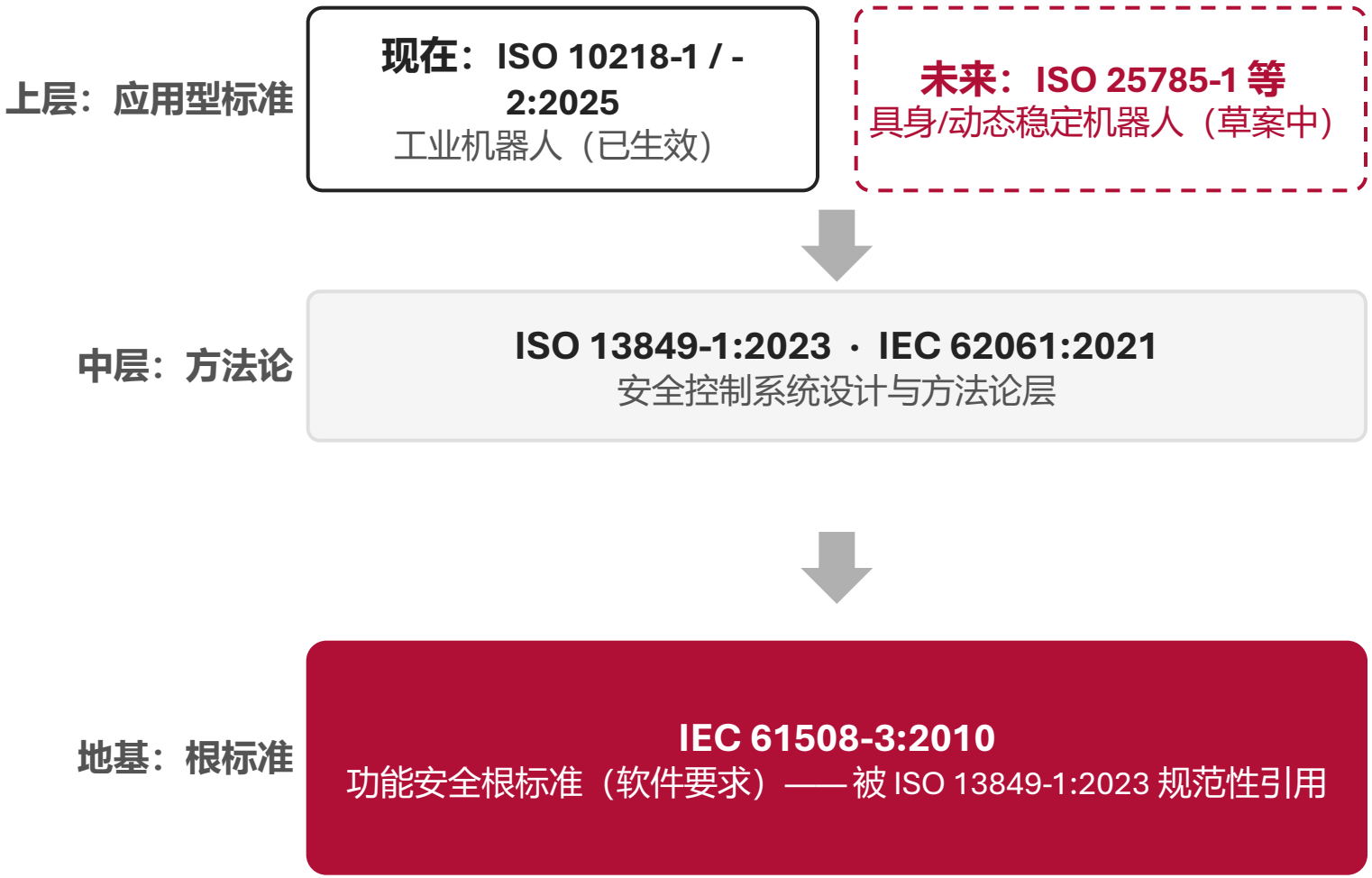
今天的设计决策，要在明天的标准下站得住。

制定中：暂不可作为当前合规依据

- ISO 25785-1：动态稳定机器人（CD，仅限工业环境）
- ISO 26058-1：工业移动机器人（WD，早于 CD）
- GB《人形机器人安全要求》5 个部分（2026 立项，起草中）
- GB 11291.1 / .2 修订（2026 立项，起草中）
- 针对新机械法规的 AI 要求，欧洲标准化组织至今未提交任何协调标准。
- 变的是上层标准，不变的是根标准 —— 工具要提供的证据也就不变。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

标准演进，基础不变



上层标准更迭，安全论证的基础不变 —— 对工具链的要求也就不变。

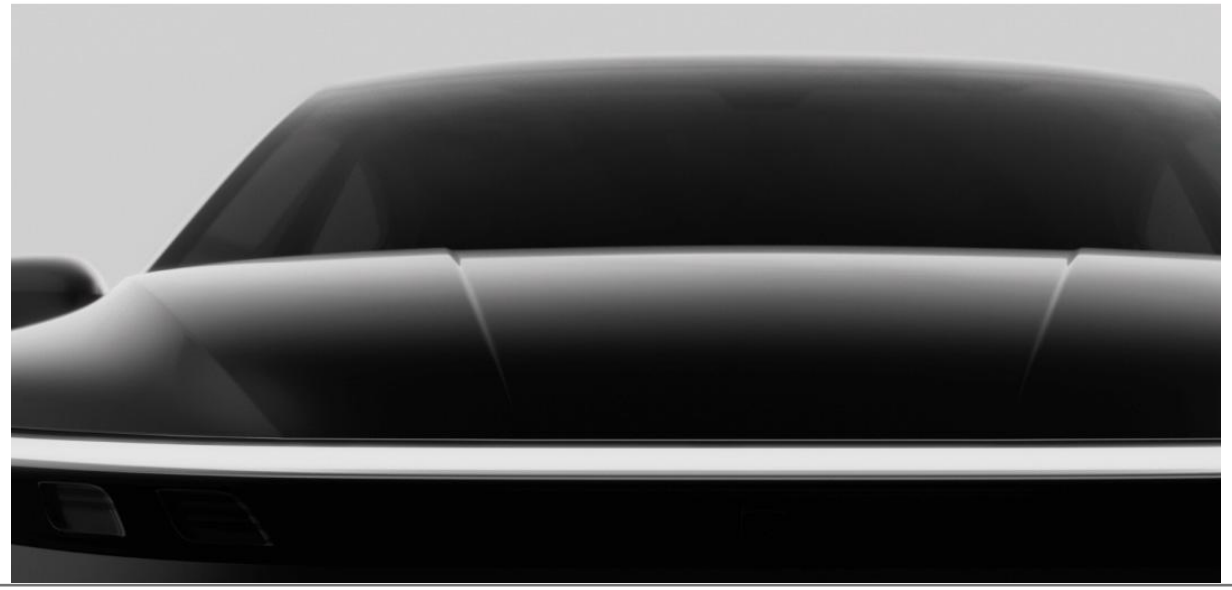
虚线 = 制定中，实线 = 已生效

Copyright © 2026 Qt Group and its group companies. All rights reserved.

02

软件工具链的四项要求





Copyright © 2026 Qt Group and its group companies. All rights reserved.

软件工具链的四项要求

01　一套工具链覆盖多种架构

对应挑战一：架构碎片化

02　工具自身具备可引用的安全资质

对应挑战二：标准碎片化

03　工具版本可长期锁定并获得支持

对应挑战三：长生命周期支持缺口

04　证据锚定根标准，可随标准演进更新

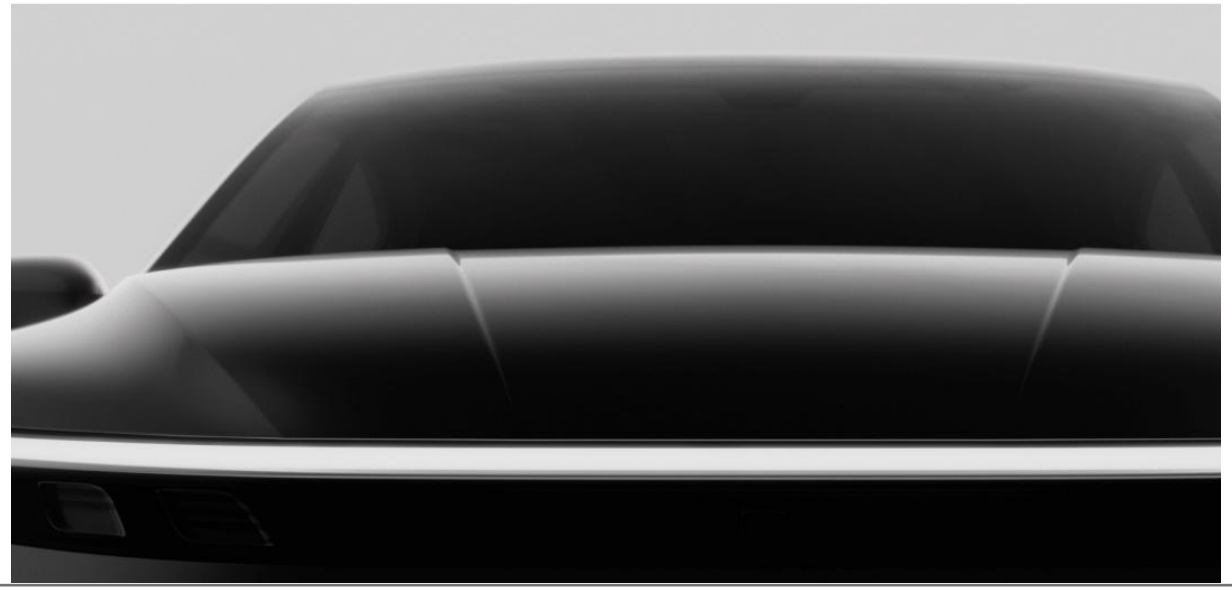
对应挑战四：标准尚未定型

Copyright © 2026 Qt Group and its group companies. All rights reserved.

03

IAR Platform 简介





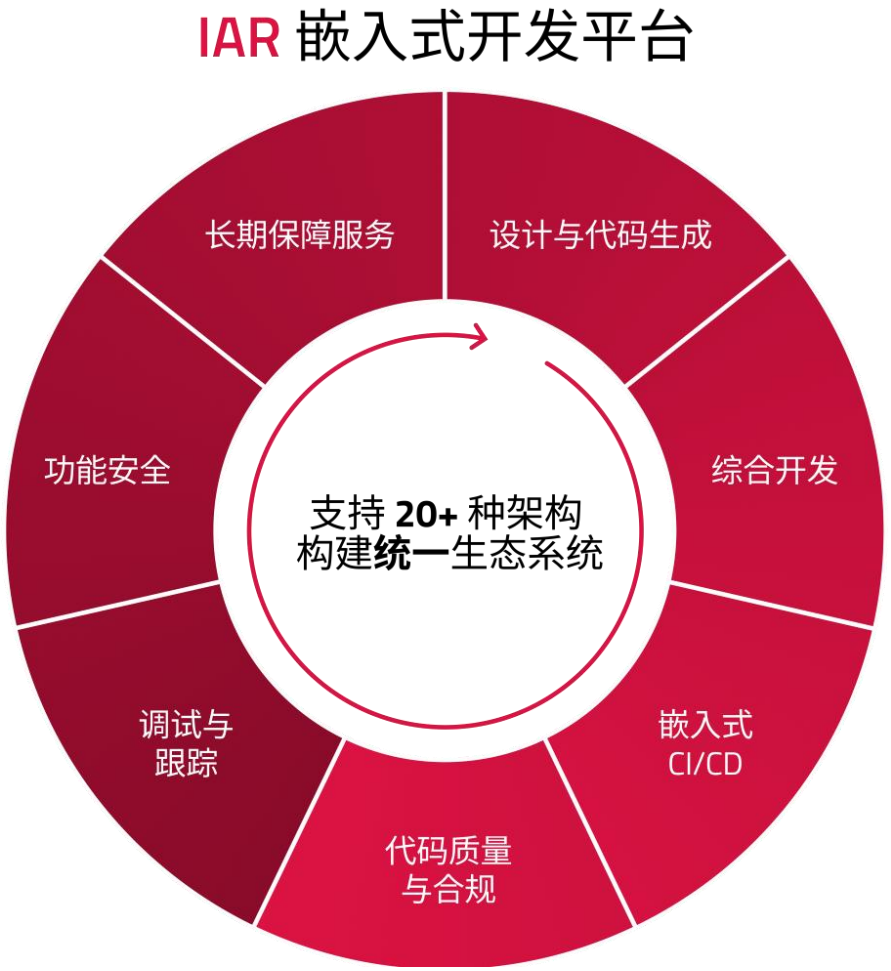
Copyright © 2026 Qt Group and its group companies. All rights reserved.

IAR Platform

IAR Platform 是嵌入式开发全生命周期工具链平台:

- **统一**：Arm/RISC-V/RH850/RX/RL78...等20多种架构的支持
- **完整**：从代码生成、编译构建、调试分析，到 CI/CD 自动化，工具链闭环覆盖整个开发周期
- **功能安全：提供 TÜV SÜD 认证版本，附带安全证书、安全报告与功能安全手册**

一次订阅即可访问 IAR 全部产品与服务。



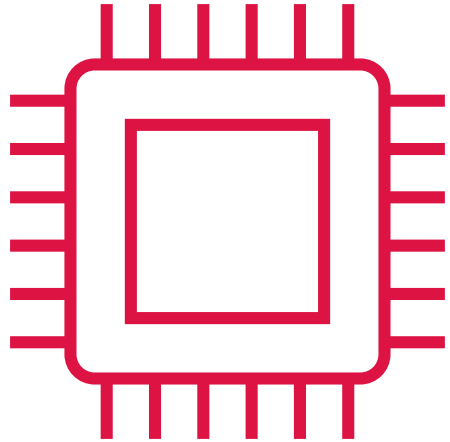
Copyright © 2026 Qt Group and its group companies. All rights reserved.

统一 Unified | 一个平台，多种架构

IAR Platform 用一套统一的平台，支持多种处理器架构：

- **20+ 架构**：Arm、RISC-V、RH850、RX、RL78、8051、MSP430 等，从 8 位到 64 位全面覆盖
- **统一工作流**：同一套风格的 IDE和构建工具，跨架构无缝切换，无需重新学习
- **一次掌握，多处复用**：减少多套工具链带来的学习与维护成本
- **平滑迁移**：加速在不同芯片间迁移和复用代码，保护既有研发投资

一个平台，覆盖你所有的目标芯片



Copyright © 2026 Qt Group and its group companies. All rights reserved.

完整 Complete｜覆盖开发全生命周期的工具链闭环

从代码到 CI/CD，IAR Platform 提供端到端的完整工具链：

- **代码生成与编辑**：IAR Embedded Workbench IDE，智能补全、代码浏览与重构
- **编译构建**：业界领先的 C/C++ 编译器与命令行 Build Tools
- **代码分析**：C-STAT 静态分析 + C-RUN 运行时分析，贯穿全程保障质量
- **调试与跟踪**：C-SPY 调试器配合 I-jet / I-jet Trace 探针，深入硬件级洞察
- **CI/CD 自动化**：Build Tools 原生支持 CI/CD，无缝接入 Jenkins、GitLab 等流水线



一个平台，从第一行代码贯通到自动化流水线

Copyright © 2026 Qt Group and its group companies. All rights reserved.

功能安全 Functional Safety｜内建认证支持，开箱即用

为安全关键应用而生，大幅降低功能安全认证的时间与成本：

- **TÜV SÜD 认证**：提供功能安全版本，附带安全证书、安全报告与功能安全手册
- **覆盖主流标准**：IEC 61508、ISO 13849、ISO 26262、IEC 62304、EN 50128 等
- **多架构支持**：Arm、RISC-V、RL78、RX、RH850、STM8
- **长期支持**：认证服务包、已知问题报告与优先技术支持

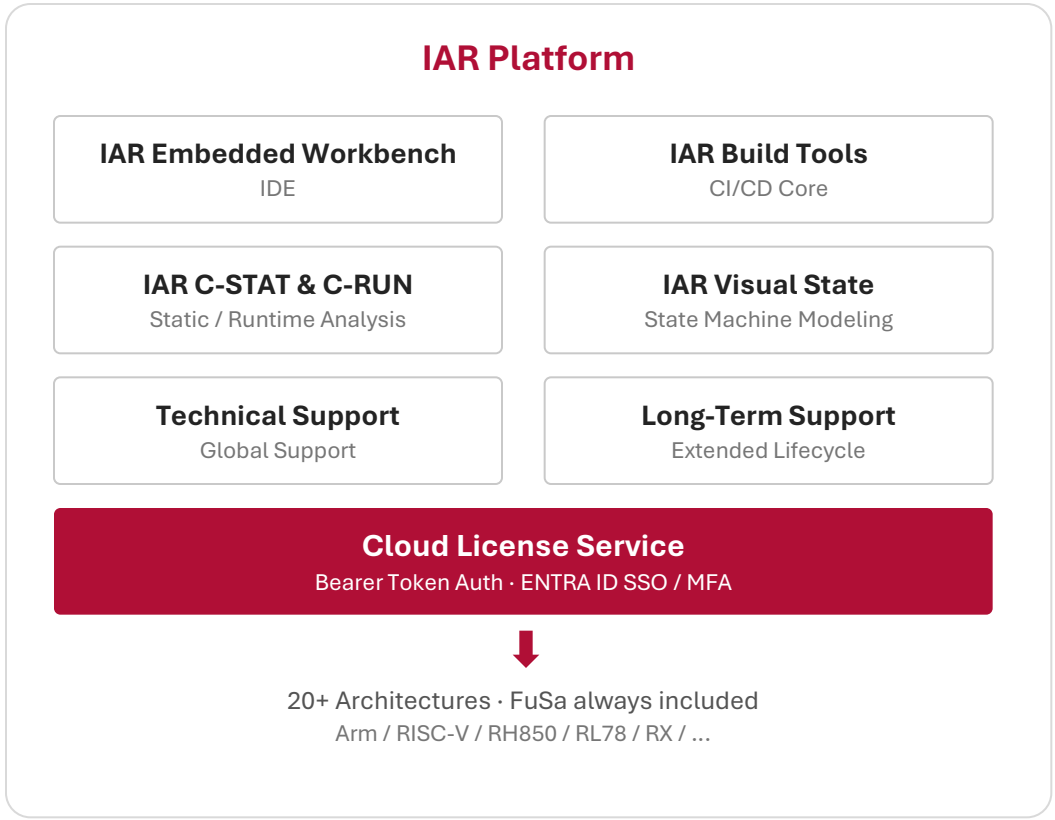
把认证负担交给工具，让团队专注产品创新



Copyright © 2026 Qt Group and its group companies. All rights reserved.

IAR Platform 产品和服务

- **产品**
  - IAR Embedded Workbench： 集成开发环境（IDE）
  - IAR Build Tools： 命令行构建 — 核心CI/CD组件
  - IAR C-STAT & C-RUN：静态分析 / 运行时分析
  - IAR Visual State：状态机建模与自动代码生成
- **服务**
  - Technical Support
  - Long-Term Support
- **云订阅授权(LMSC)**
  - 云端授权 · ENTRA ID SSO / MFA/ Bearer Token Auth
- **多架构支持**
  - 20+ 架构： Arm / RISC-V / RH850 / ...
- **功能安全内置**
  - TÜV SÜD 认证版本包含在内

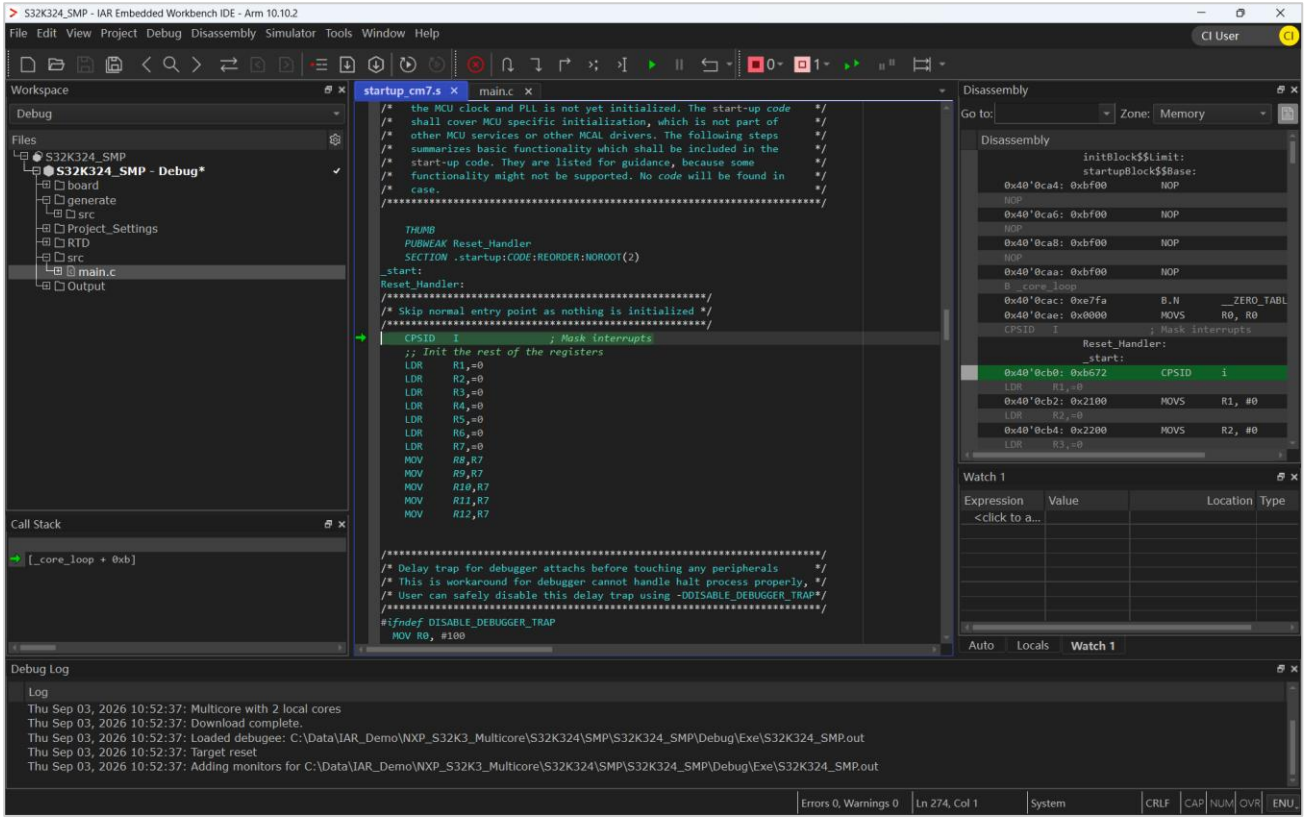


Copyright © 2026 Qt Group and its group companies. All rights reserved.

集成开发环境

IAR Embedded Workbench IDE

- 用户友好
  - 能够管理一个简单项目到多项目工作区，并配备多种配置
  - 源代码浏览器
  - 代码补全
  - 语法重点
- 代码分析包含
  - 静态代码分析
  - 运行时分析
- 综合调试
- 跨平台支持
  - 原生支持Linux/Windows
- Free trial available



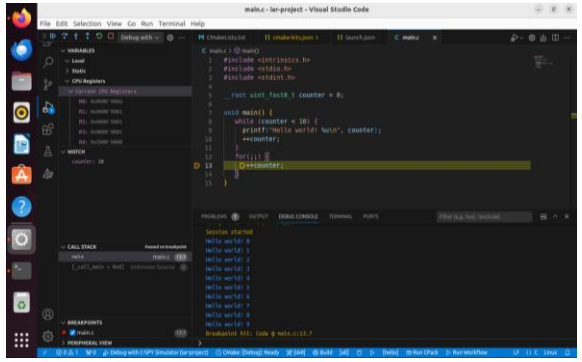
Copyright © 2026 Qt Group and its group companies. All rights reserved.

Visual Studio Code 的 IAR 扩展

IAR Embedded Workbench, IAR Build Tools

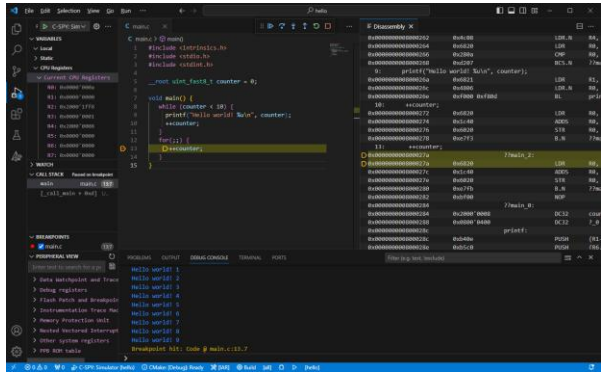
IAR Build

- 用于 IAR Embedded Workbench 项目（*.ewp）
- 管理项目文件
- 使用 IAR C-STAT 进行静态代码分析
- VS Code 和 IAR Embedded Workbench 间快速切换



IAR C-SPY Debug

- 调试以下方式构建的可执行文件
  - IAR project format (*.ewp), CMake, Makefiles, etc.
- 原生 IAR C-SPY support
  - Built-in simulator
  - Multi-core debugging
  - RTOS thread awareness



Copyright © 2026 Qt Group and its group companies. All rights reserved.

CI/CD工作流的理想解决方案

IAR Build Tools

- 命令行工具
  - 完整嵌入式工具链
  - 非交互式调试器（用于自动化测试）
    - Simulator, IAR I-jet, SEGGER J-Link
- 代码分析包含
  - IAR C-STAT（静态代码分析）
  - IAR C-RUN （运行时分析）
- 跨平台
  - Linux（Ubuntu 或 Red Hat ）
  - Windows（10及以上版本）
- 可部署于典型的CI/CD环境中
  - Self-hosted
  - Cloud-hosted

```
# Build
> iarbuild project.ewp –build Release
[...]
Total number of errors: 0
Total number of warnings: 0

Build succeeded


# Static Code Analysis (C-STAT)
> iarbuild project.ewp –cstat_analyze Release
[...]

Analysis completed. 128 message(s)


# Runtime Analysis (C-RUN)
> CSpyBat ... --rtc_enable --debug-file=/path/to/executable.out
[...]

CSpyBat terminating.


# Flash the target
> CSpyBat ... --download_only --debug-file=/path/to/executable.out
[...]

CSpyBat terminating.
```

Copyright © 2026 Qt Group and its group companies. All rights reserved.

Qt Group

功能安全

IAR Embedded Workbench – Functional Safety Edition
IAR Build Tools – Functional Safety Edition

支持架构

- Arm
- RISC-V
- Renesas RL78
- Renesas RX
- Renesas RH850
- ST STM8

简化验证

- TÜV SÜD 功能安全证书
- TÜV SÜD 功能安全报告
- IAR 功能安全手册



长期支持（LTS）

- 认证服务包
- 已知问题报告
- 优先技术支持



Copyright © 2026 Qt Group and its group companies. All rights reserved.

功能安全
Standards

	Industrial	Automotive	Railway	Medical	Agriculture & Forestry	Machinery Control	Process Industry	Household Appliances
	IEC 61508	**ISO 26262**	**EN 50128 EN 50657**	**IEC 62304**	**ISO 25119**	**ISO 13849 IEC 62061**	**IEC 61511**	**IEC 60730**
Arm	●	●	●	●	●	●	●	●
RISC-V	●	●	●	●	●	●	●	●
Renesas RL78	●	●	●	●	●	●	●	●
Renesas RX	●	●	●	●				
Renesas RH850	●	●	●	●				
ST STM8	●	●	●	●				

Copyright © 2026 Qt Group and its group companies. All rights reserved.

长期支持与维护

LTS, Limited LTS & Maintenance License

LTS 与 Limited LTS

- LTS：验证过的 Service Pack、已知问题报告、优先技术支持
- Limited LTS：内容相同，但不提供 Service Pack 与补丁
- 服务期 1–5 年可续约，合约支持最长可达 10 年
- Maintenance License 包含在 LTS 内

选定的「proven in use」版本获得认证；Service Pack 为累积式，含安全相关缺陷修复。

Maintenance License

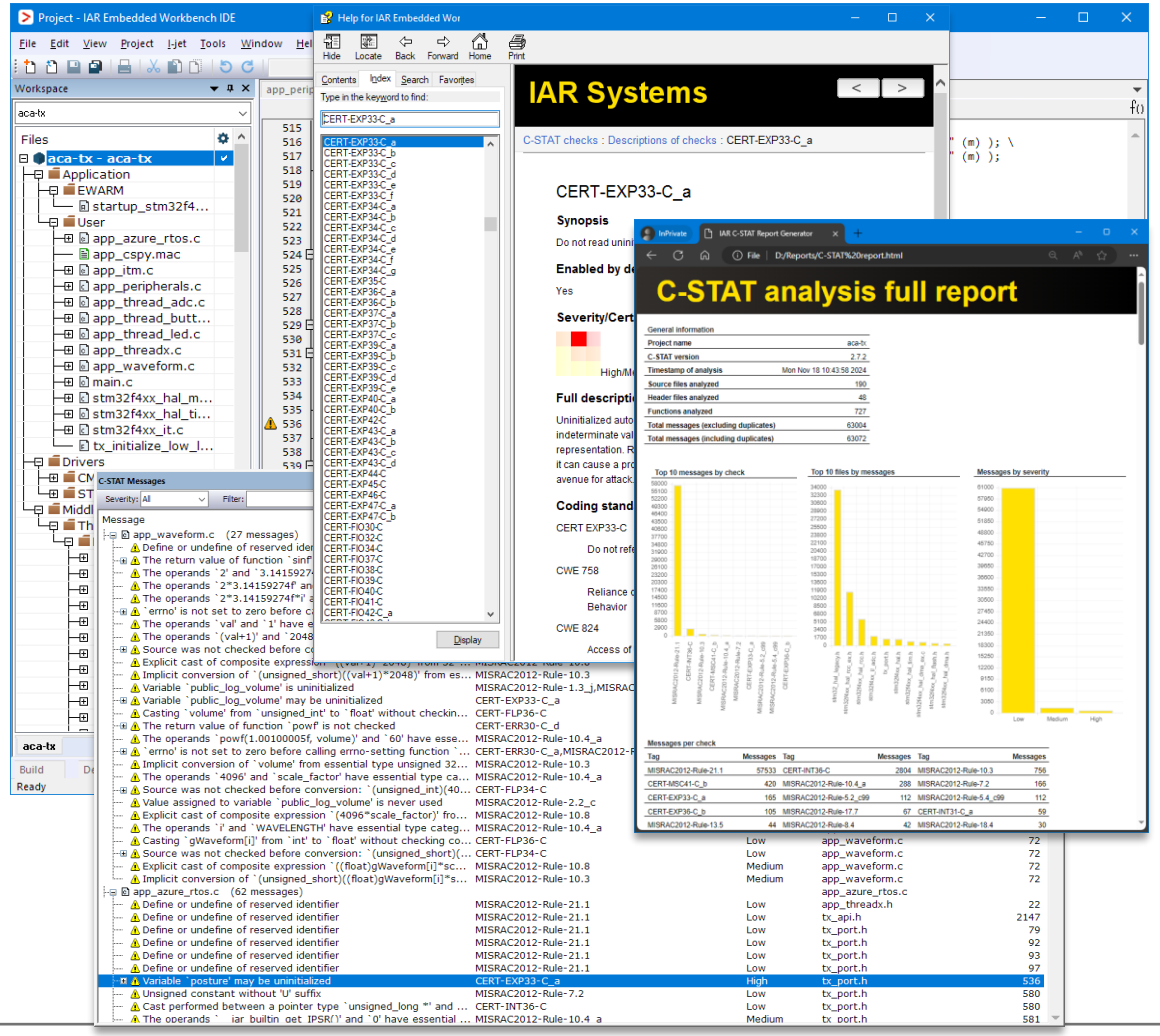
- 面向 10–20 年质保周期的客户
- 永久使用特定版本的权利，仅限维护
- 只做维护与缺陷修复，不启动新项目
- 可与 LTS 服务组合，获得长期稳定性

Copyright © 2026 Qt Group and its group companies. All rights reserved.

静态代码分析

IAR C-STAT

- 确保整个开发周期的 C 和 C++ 代码质量
- 检查规范合规性
  - MISRA C (2023, 2012, 2004)
  - MISRA C++ (2023, 2008)
  - SEI CERT C (Secure Coding)
  - CWE (Common Weaknesses Enumeration)
- 详细列表，带有上下文相关帮助
- 完整分析报告生成
- **TÜV SÜD认证版本**
  - Arm, RISC-V and Renesas RH850, RL78

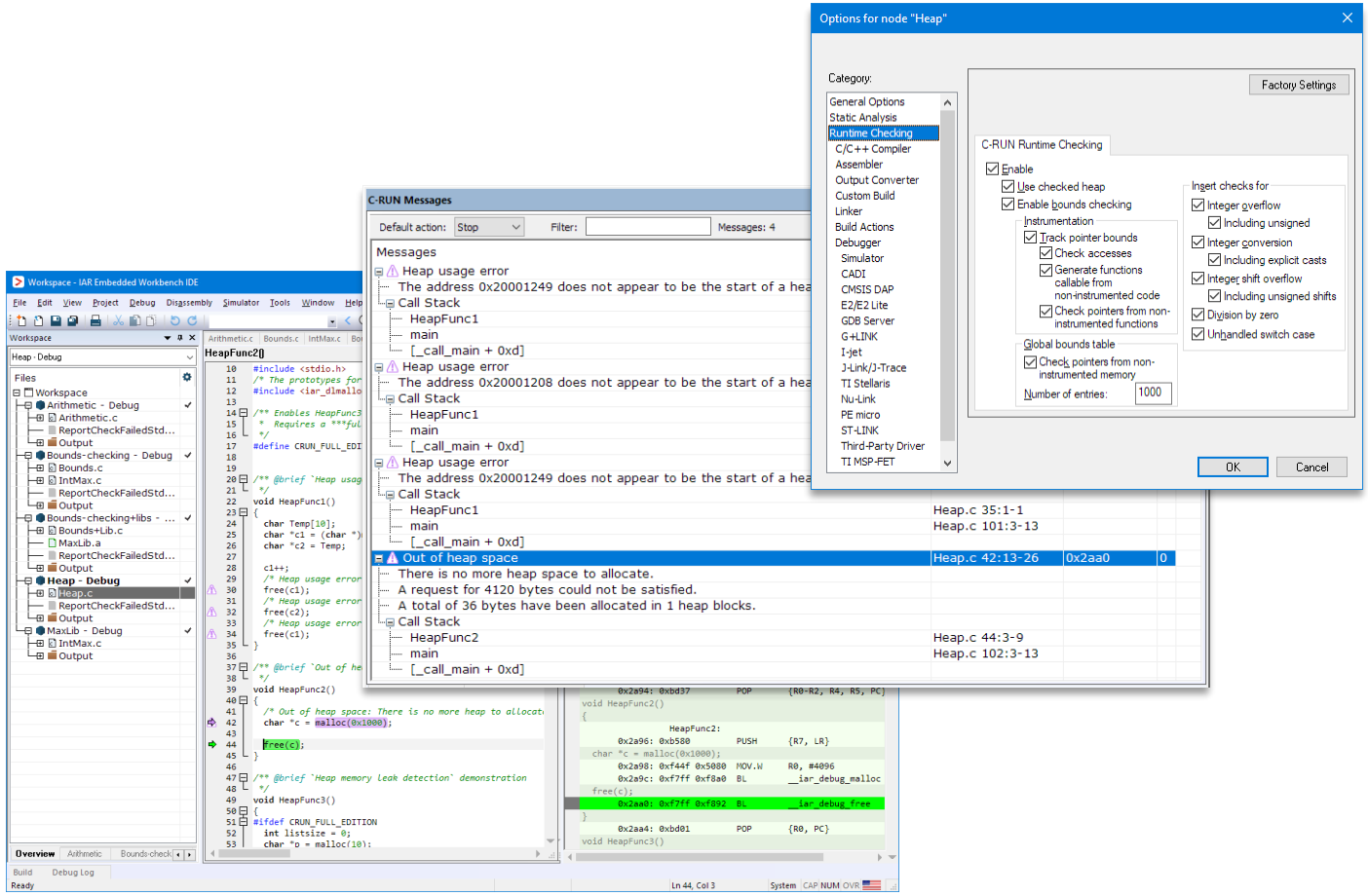


Copyright © 2026 Qt Group and its group companies. All rights reserved.

运行时分析

IAR C-RUN

- 快速检测可预防的错误，如
  - Bit losses in shifting operations
  - Buffer overflow
  - Division by Zero
  - Heap memory corruption and leaks
  - Out-of-bounds access for arrays and objects
  - Type casting inadvertent value changes
- 适用于Arm和Renesa RX
- Github上提供评估指南 [hands-on guide]



Copyright © 2026 Qt Group and its group companies. All rights reserved.

全面的调试体验

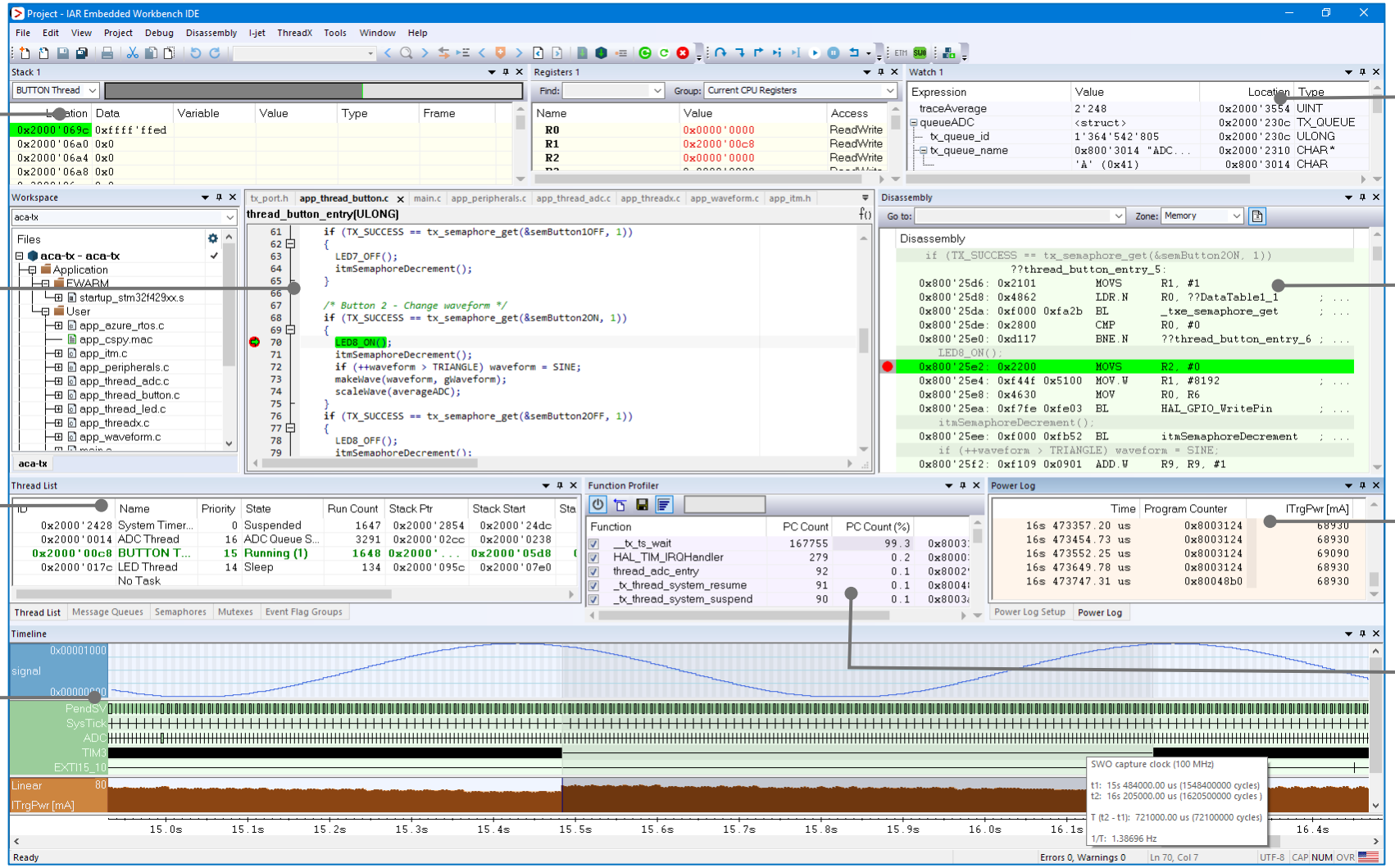
IAR C-SPY Debugger

Stack monitor
Thread-specific
CSTACK

Code Editor
Edit source code while in the debugging session

RTOS Awareness
ThreadX
FreeRTOS
Mbed and more

Timeline
Track runtime application behavior



Viewers
Registers
Variables
Live updates

Disassembly
For deeper, low-level debugging

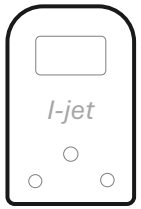
Power usage
Log power consumption

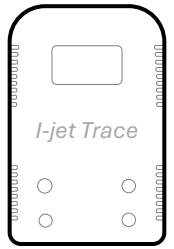
Function Profiler
For deeper performance analysis

Copyright © 2026 Qt Group and its group companies. All rights reserved.

硬件仿真调试器

IAR Debug and Trace probes





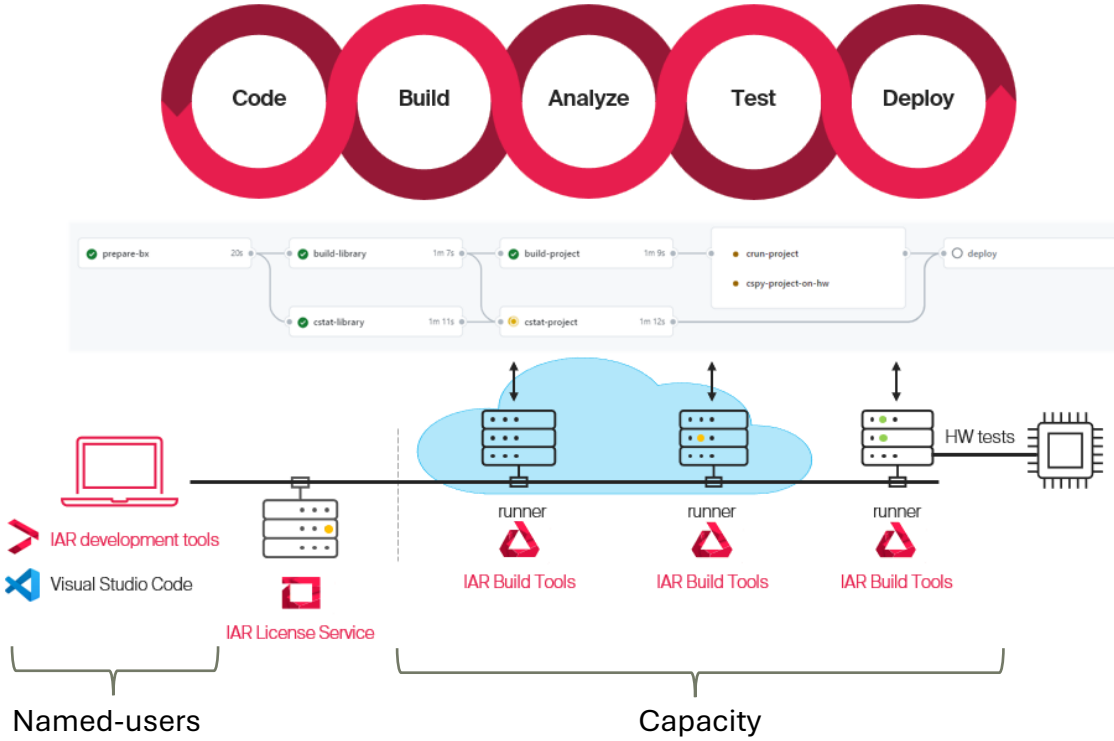
	I-jet	I-jet Trace
Core support	**Arm Cortex(-M,-R,-A)[1], RISC-V[2]**	
Host interface	USB 2.0	USB 3.0
Target Powering Option (max.)	5V/420 mA	5V/600 mA
Power Debugging	**160 µA @ 200 kSPS**	
Debugging Interfaces	JTAG, SWD	JTAG, SWD, ETM
Serial Wire Output (SWO)	30 Mbps	60 Mbps
Code Coverage	Sampled	Full
Embedded Trace Macrocell (ETM)	-----	(up to) 16-bit wide @ 350 MHz
Flash breakpoints	**Unlimited**	

[1] when using with IAR Embedded Workbench for Arm
[2] when using with IAR Embedded Workbench for RISC-V

Copyright © 2026 Qt Group and its group companies. All rights reserved.

云订阅授权： LMSC for IAR Platform

- IAR Platform 从按机器授权产品，转向按**人员**和**流水线**授权访问
- LMSC： License Management System Cloud
- 一个平台，两个维度:
  - Named-User — 面向开发者
  - Capacity — 面向 CI/CD 流水线
- 涵盖了嵌入式开发的每一个阶段，从代码的第一行到CI/CD流水线运行
- 更优的灵活性与可扩展性。无需针对单个产品或架构的特别决策



Copyright © 2026 Qt Group and its group companies. All rights reserved.

从第一行代码到生产： IAR Platform 全流程覆盖



Design + Verify + Generate code

直观的图形建模
IAR Visual State 简化可视化状态设计，用于基于状态机的建模与验证.

验证与代码生成
通过IAR Embedded Workbench自动化并确保代码正确性，优化代码生成。

Code + Test + Build + Debug

提高代码质量& 降低缺陷风险
使用IAR Embedded Workbench和IAR C-STAT/C-RUN高效优化和调试您的应用。

快速调试和广泛的设备支持
使用I-jet/I-jet Trace 加快调试，并利用工具支持Arm和RISC-V的生态系统兼容性。

始终包含功能安全
使用 IAR Embedded Workbench for Functional Safety 满足功能安全的要求.

CI/CD Build + Test

自动化工作流程与DevOps实践
使用IAR Build Tools集成CI/CD流水线进行自动化构建，并使用IAR C-STAT 和 C-RUN 进行测试。

成本控制与优化开发
通过支持构建自动化工具的IAR工具，确保代码和资源效率的优化。

始终包含功能安全
通过IAR 命令行工具的功能安全版实现安全合规自动化。

Release

合规证据自动生成
每次发布自动产出可供审计的文档，覆盖 CRA 与功能安全认证的要求。

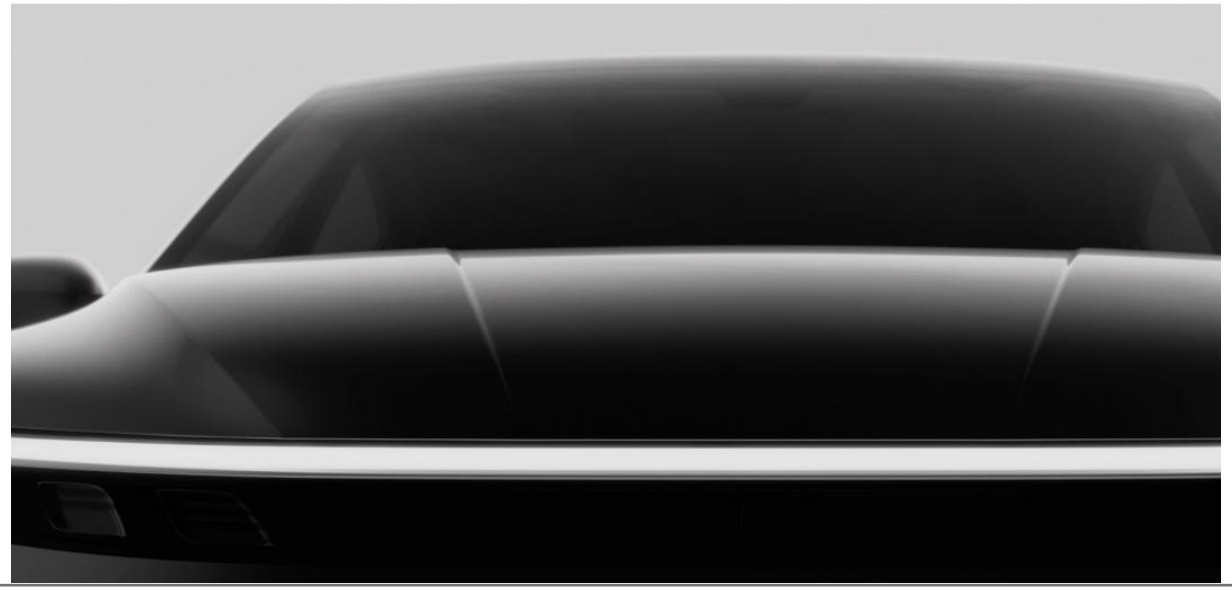
可复现的长周期发布
每一次发布构建都可从源码复现，多年后仍能重新生成当初出厂的固件，用于审计或现场问题追溯。Long-Term Support Services 让认证过的工具链与构建环境保持稳定，今天的发布无需重新验证即可长期有效。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

04

总结





Copyright © 2026 Qt Group and its group companies. All rights reserved.

总结：四类挑战，一条逻辑线

01

架构碎片化 → 工具链碎片化

应对：一个平台覆盖多种架构，编译、分析、调试与认证证据结构统一

02

标准碎片化但归一

应对：一条可追溯的证据链，指向 IEC 61508-3

03

长生命周期支持

应对：长期支持（LTS）、已知问题报告与认证版本对照，长周期内可复现

04

标准仍在演进

应对：证据链锚定 IEC 61508-3 与认证工具基座，新标准落地不必推倒重来

上层标准持续演进，安全论证的基础不变；IAR Platform 提供的是这一基础上的工具与证据。

Copyright © 2026 Qt Group and its group companies. All rights reserved.

资料下载

白皮书：《在现代嵌入式开发中，降低生命周期风险》



由 VDC Strategy 独立完成的研究报告，基于对 600 多位产品决策者和工程师的调研，深入剖析了究竟是什么在真正拖延项目进度、加剧合规压力，以及割裂的工具链背后隐藏的成本。您将了解到：

- 为什么合规正成为嵌入式团队采购决策中的首要考量因素
- 割裂的工具链，在产品整个生命周期内究竟会带来多少隐形成本
- 架构灵活性（Arm、RISC-V 等）如何影响长期风险
- 一个真正面向未来十年、而不只是面向下一次版本发布的嵌入式开发平台，应该具备哪些特质

扫码下载

Copyright © 2026 Qt Group and its group companies. All rights reserved.

Contact: Brendan.pan@qt.io



Qt Group | Qt | iar | squish | Axivion | coco