Safety and Security: The Cornerstones of QNX

聚焦QNX的基石：功能安全与网络安全

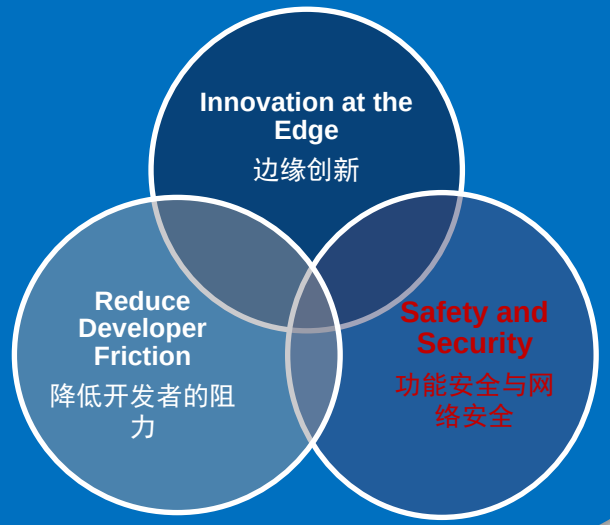
Harry Yu
Senior Director, Engineering Services - APAC

BlackBerry QNX Overview | BlackBerry QNX 简介

概述

- 凭借四十多年经验，提供客户关键嵌入式系统的基础软件，获得广泛信任与验证
- 为汽车OEM、Tier 1供应商以及通用嵌入式市场提供操作系统、hypervisor（虚拟机监视器）、开发工具和技术支持服务
- 因获得最高级别的安全与认证而广受认可
- 在汽车行业中，作为安全认证、可靠性和安全性软件的行业领导者

产品组合概览



关键市场分布

Automotive 汽车行业

255M+

Vehicles

- Industrial Automation 工业自动化
- Medical Devices 医疗器械
- Robotics 机器人技术
- Commercial Vehicles 商用、特殊车辆

Diverse Customers/Partners Across Industries
跨行业的多样化客户/合作伙伴

gm, aws, BMW, BOSCH, Continental, DENSO, DFM, Ford, GE, VW, Google, HONDA, Itron, JAGUAR, LAND ROVER, LG, LUCID, Medtronic, Mercedes-Benz, NVIDIA, Panasonic, Qualcomm, STELLANTIS, synaptics, Texas Instruments, TOYOTA, Visteon, VOLVO, Baidu 百度

BlackBerry | QNX

Cybersecurity vs Safety | 网络安全与功能安全的对比

- 网络安全与功能安全紧密相连，互相依赖
- 功能安全性是网络安全需求的主要驱动力之一
- 在产品生命周期中，都采用类似的V模型
- 根本性的差异:

	Cybersecurity 网络安全	Safety 功能安全
范围	系统的所有部分都在范围之内，在网络安全领域尚无混合关键性概念	在混合关键性系统中，功能安全要求通常仅限于系统的某个小部分
关注事项	恶意尝试破坏系统完整性，数据泄露	系统故障导致人员和财产损失
静态/动态	动态： 运行系统的网络安全态势不断变化（需要实时监测、更新和响应攻击）	静态：在开发和设计阶段注重系统架构、失效模式和冗余，功能安全措施预计随着时间的推移保持不变
产品生命周期的影响	安全漏洞监控必须在系统运行期间持续进行	安全缺陷监控通常在产品生命周期结束时终止

ISO 26262 道路车辆功能安全标准

- **背景和目标**
  - 功能安全的扩展和具体化标准：专门针对道路车辆的复杂电子和电气（E/E）系统。
  - 系统化的风险管理流程：确保电子系统的功能在发生故障时能够最大限度地降低对人身安全的影响。。

- 关键概念
  - ASIL（Automotive Safety Integrity Level）：
    通过风险评估将安全要求划分为四个等级（A、B、C、D），其中 ASIL D 是最高的安全要求。
  - 安全生命周期（Safety Lifecycle）：
    从概念到产品退役的一整套流程，确保系统开发和运行符合安全标准。
  - 验证与确认（Verification and Validation）：
    强调对功能安全要求的测试、审查和确认，确保系统满足安全需求。

- 行业意义
  - **风险控制**：提供了一种系统化方法，帮助开发团队评估并控制功能失效风险。
  - **合规性需求**：是许多国家和地区汽车行业法规的基础，用于满足监管要求。
  - **推动技术发展**：引导开发人员在设计中更深入地考虑安全问题，推动安全性和可靠性技术的进步

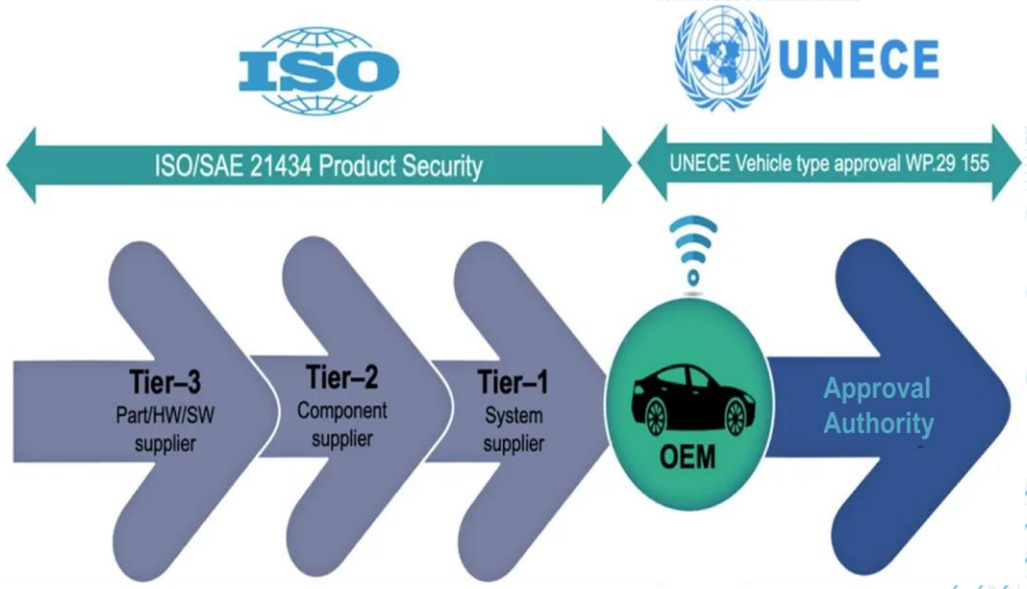
Standardization for Vehicle Cybersecurity WP.29 & ISO 21434

车辆网络安全标准化 – WP.29 和 ISO 21434

- WP.29 R155是由联合国欧洲经济委员会（UNECE）于2021发布的法规
  - **网络安全管理系统（CSMS）**：要求车企建立一个正式的 CSMS，用以持续管理网络安全风险。
  - **安全设计要求**：确保车辆在设计时就考虑到网络安全（“安全即设计”）。
  - **风险评估（TARA）**：要求车企对潜在网络安全威胁进行评估和缓解。
  - **漏洞和事件响应**：能够检测、报告和应对安全事件。
  - **安全更新**：确保通过 OTA（空中下载）或其他方式提供安全更新，同时保障车辆功能安全

- **符合WP.29 R155是获得“车辆类型”批准的前提条件**，适用于60多个国家的OEM
  - 2024/2025年（欧洲），2022/2023年（日本和韩国），2022年（中国），（待定）加拿大/美国
  - **适用于OEM及其供应商**，涵盖四轮以上车辆的所有电子/电气(E/E)系统和整个车辆生命周期的各个阶段。

- **ISO 21434 是网络安全标准，与WP.29 R155标准对接。**
  - **ISO 21434** 提供了详细的指导（“如何(how)”）— 认证标准
  - **WP.29 R155** 关注于要求（“什么（what)”）— 法律约束



ISO 21434 Certification Activities
ISO 21434 认证方面取得的进展

- QNX拥有成熟且值得信赖的质量管理体系（QMS）
  - 已通过多个行业标准的功能安全和网络安全性测试
  - 成功通过了多个OEM客户的审计。
- QNX积极参与了ISO 21434标准的制定。
- QNX流程已获得ISO 21434 ML2认证。
- 未来发布的QNX产品将会根据ISO/SAE 21434 ML3进行认证。
- QNX将通过参与供应商认证评估的活动、提供项目交付所需的材料（如网络安全接口协议）等方式，支持客户实现WP.29和ISO/SAE 21434的合规性。

Certificate

Cyber Security Management

Automotive CS Management (TÜV Rheinland)
ISO/SAE 21434 - Automotive Tier Supplier
ACSM 129, Maturity Level 2: Managed

Certificate No. 968/ACSM 129.00/24

Certified Company & Location
BlackBerry Limited
1001 Farrar Road
Ottawa, ON K2K 0B3
Canada

Scope of Certification
Automotive Tier 1 / 2 Supplier
according to
ISO/SAE 21434:2021 - Road Vehicles-Cybersecurity Engineering
based on
Clause 4 - General Considerations
Clause 5 - Organizational Cybersecurity Management
Clause 6 - Project dependent Cybersecurity Management
Clause 8 - Continual cybersecurity activities
Clause 9 - Concept
Clause 10 - Product development
Clause 13 - Operation and maintenance
Clause 14 - End of cybersecurity support and decommissioning
Clause 15 - Threat analysis and risk assessment methods

Achieved **Maturity Level: ML2 - Managed**

The Certified Company has successfully demonstrated during an audit process that an Automotive Cybersecurity Management System has been defined and implemented. It will be applied in the concept design, development, operation and maintenance of commercial operating systems, hypervisors, development tools, support and services, all purpose-built for the world's most critical embedded systems.

Purpose of the audit is to obtain evidence of compliance with the organizational requirements related to **Automotive Cybersecurity Management Processes** according to the Scope of Certification.

This ACSM Certification only refers to the listed company location and their involved departments, which comply with the organizational requirements for the listed Scope of Certification. It does not replace any kind of product specific confirmation measures including product specific audits, assessments or according certifications.

Validity This certificate is valid until 2025-06-14

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2024-06-14

Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see https://www.tuvasi.com. The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT CMP V1.0:2020 in its actual version, whose results are documented in Report No. 968/ACSM 129.00/24 dated 2024-05-13. Issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-00.

Executive Order 14028 & SBOM (Software Bill of Materials)
行政命令14028和软件物料清单

- **行政命令14028（EO 14028）于2021年5月发布**
  - **实施国家**：主要适用于美国境内的联邦机构、供应商以及与政府合作的私营部门公司。
  - **国际影响**：虽然是美国政策，但由于它对软件供应链安全提出严格要求，对跨国企业（尤其是向美国政府提供服务的企业）也可能产生间接影响。
  - **关键要求**：要求企业采用更高的网络安全标准，并提供 SBOM 以确保透明的供应链安全

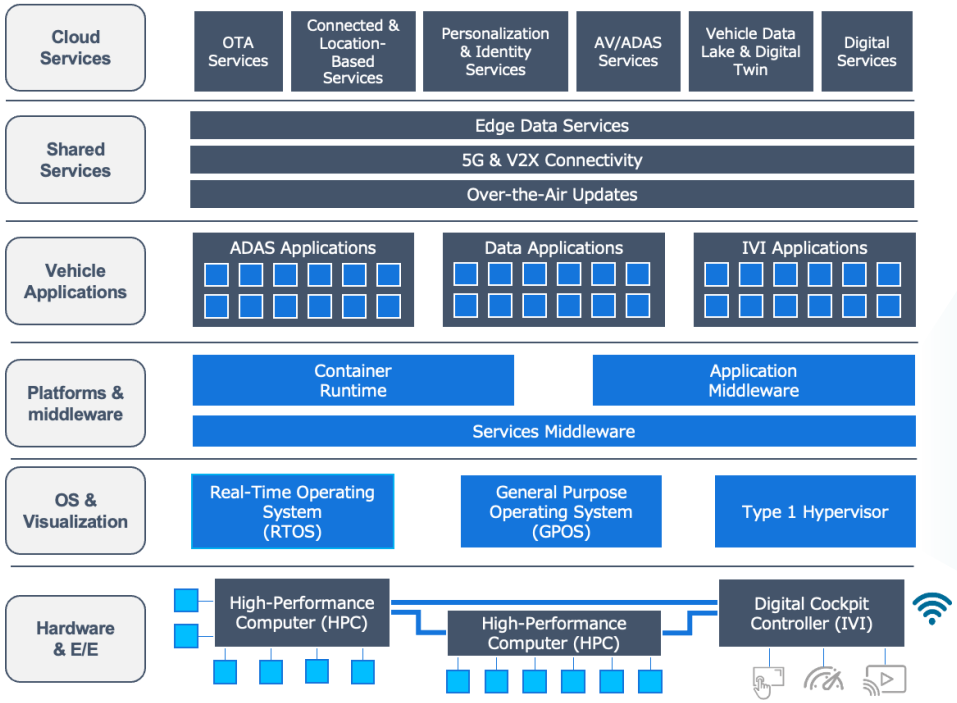
- **SBOM主要采用国家**：目前 SBOM 的应用范围集中在美国，但它的概念正逐渐被其他国家和地区所接受，包括：
  - **欧盟**：通过《网络韧性法案》（CRA）等政策鼓励企业采用类似 SBOM 的透明化措施。
  - **日本和韩国**：因供应链安全问题，也逐步开始关注类似标准。
  - **全球范围**：跨国企业，如软件开发公司和云服务供应商，可能会因向美国或其他法规要求类似透明度的市场出口而采用 SBOM。

SBOM 作为一种全球网络安全趋势，可能在未来被更广泛的国家和地区采纳，尤其是随着供应链攻击事件的增多。

BlackBerry QNX Software Product Portfolio
BlackBerry QNX 产品组合概览

BlackBerry QNX的基础软件产品和专业服务致力于帮助客户构建基于QNX的产品系统，同时确保不妥协功能安全性、网络安全性，可靠性或稳定性。

Next Gen Automotive SDV Architecture



BlackBerry QNX Software Product Portfolio

功能安全认证与服务

ISO 26262
IEC 61508
IEC 62304
EN 50128
EN 50657

- QNX Cloud Enablement
- QNX Frameworks and core add-ons — *Cabin, QNX Sound, Sensor Fmwk*
- QNX Operating System
- QNX Hypervisor
- QNX Software Development Tools

网络安全软件、工具与服务

Crypto, PKI, Cert Mgmt, Code Signing, SBOM, Incident Response

FIPS
WP.29
ISO 21434
CC 15408

BlackBerry QNX Global Professional Services

Certified Products & Services | 安全认证的产品和服务

	ISO 26262	IEC 61508	IEC 62304	EN 50128	EN 50657
PRODUCTS					
QNX OS for Safety	✓	✓	✓	✓	✓
Safety-Certified C++ Library	✓				
QNX Hypervisor for Safety	✓	✓	✓	✓	✓
QNX Comms for Safety	✓				
QNX File System for Safety	✓				
QNX Encryption for Safety *(upcoming)*	✓	✓	✓		
QNX Graphics Safety Monitor	✓				
SERVICES					
Safety Training	✓	✓	✓	✓	✓
Safety Audit	✓	✓	✓	✓	✓
Safety Software Development	✓	✓	✓	✓	✓
Safety-Certified BSP Startup	✓	✓	✓	✓	✓
Safety-Certified BSP Components	✓	✓	✓	✓	✓
Safety Architecture Consultation	✓	✓	✓	✓	✓
Safety Workshops	✓	✓	✓	✓	✓

Significant Progress Against Strategic Roadmap Priorities
产品规划的显著进展

边缘创新

QNX 8.0 Commercial Release

- 交付了高性能可扩展的实时操作系统，以支持客户的先进开发需求
- 在大规模部署下提升了性能，支持64核及以上处理器
- **QNX 8.0 Hypervisor**
- 客户提前体验和测试版本的发布

Virtualization Support via VirtIO Standards Contributions

BlackBerry IVY GA Release

聚焦–功能安全与网络安全

Safety Enhancements

- 提供了行业首个安全认证的虚拟化框架
- 交付了针对特定行业的安全操作系统版本（汽车、工业、医疗、铁路）
- 发布了安全认证至最高级别的C++运行时环境

Security Upgrades

- 增加了网络安全分析和事件响应团队
- 获得ISO 21434认证
- 创建了支持汽车制造商WP.29合规性的服务

降低开发者的阻力

Cloud Enablement

- 在云端发布了QNX操作系统、安全认证的操作系统和hypervisor 虚拟机管理监控器

Open-Source Project Support

RUST Programming Language

- 在QNX上提供支持，并上传到开发社区

Partner Integrations

- 增强了QNX-ready软件集成（eAVB、Autosar、音频等）
- 扩展了硬件支持

提供面向未来的软件产品组合，以推动无与伦比的创新和客户价值。

Enabling Innovation at Scale in 2024 and Beyond
2024年及以后大规模创新的实现

边缘创新

QNX 8.0 Portfolio Expansion

- 开发高附加值的扩展产品，例如容器(container)、虚拟化扩展、复杂调度(scheduling)支持
- 在多个芯片供应商平台上发布商用的Hypervisor 8.0
- 与合作伙伴提供预集成的平台和领域解决方案
- 支持下一代高性能芯片和板卡

Software-defined audio products

Microcontroller and RISC-V 支持的技术评估

聚焦–功能安全与网络安全

Safety Enhancements

- 交付QNX 8 safety OS 安全操作系统、QNX 8 safety hypervisor, 和safety containers
- 扩展安全认证软件产品组合和专业服务
- 发布针对汽车和通用嵌入式的C++资格认证工具包

Security Upgrades

- 交付软件物料清单（Software Bill of Materials）及ISO 21434合规服务
- 推出入侵与异常检测的监控与审计框架

降低开发者的阻力

QNX Everywhere

- 启动推广项目以大幅扩展 QNX 开发者社区的规模。

Open-Source Project Support

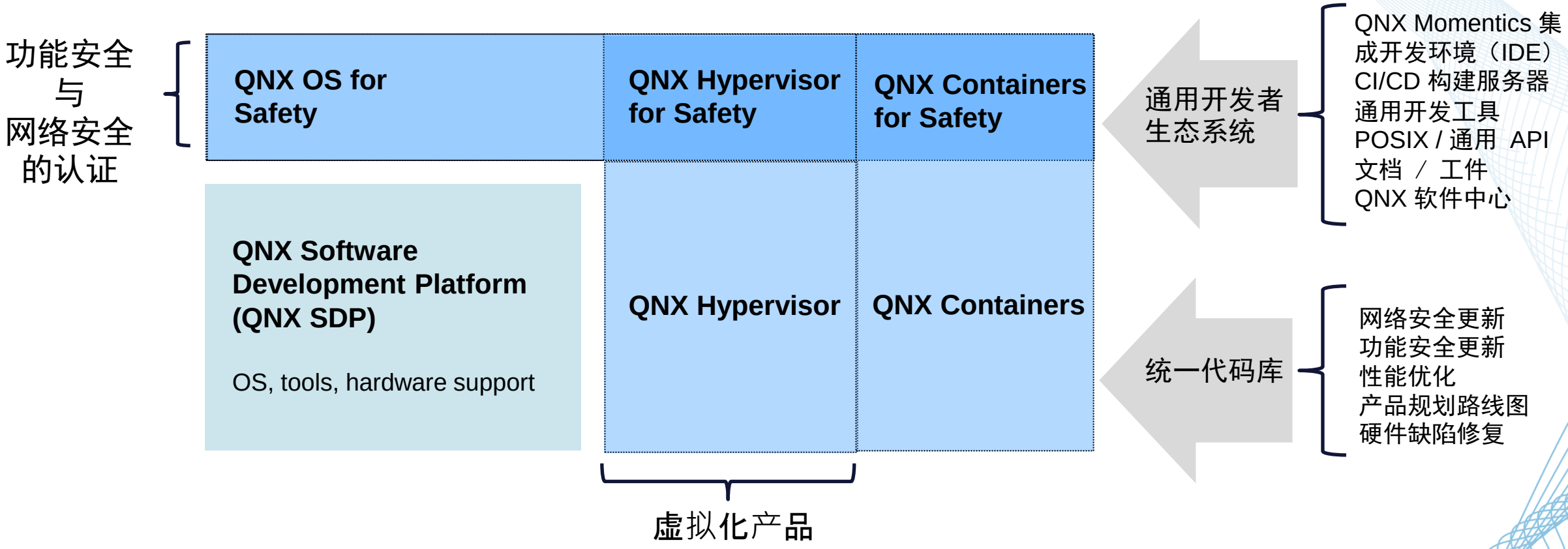
- 移植、优化并维护更多开源项目。

Cloud Enablement

- **云优先工具战略：**优先开发基于云的开发工具
- **云产品支持：**包括 QNX 8 操作系统、安全产品、虚拟化和平台的云功能支持
- **虚拟 ECU**（电子控制单元）支持
- 支持更多的云端供应商并加强协作。

基于我们在性能、安全性、可靠性和安全方面的卓越声誉

Unified Code Base with Interchangeable Safety Levels
统一的软件代码的优势



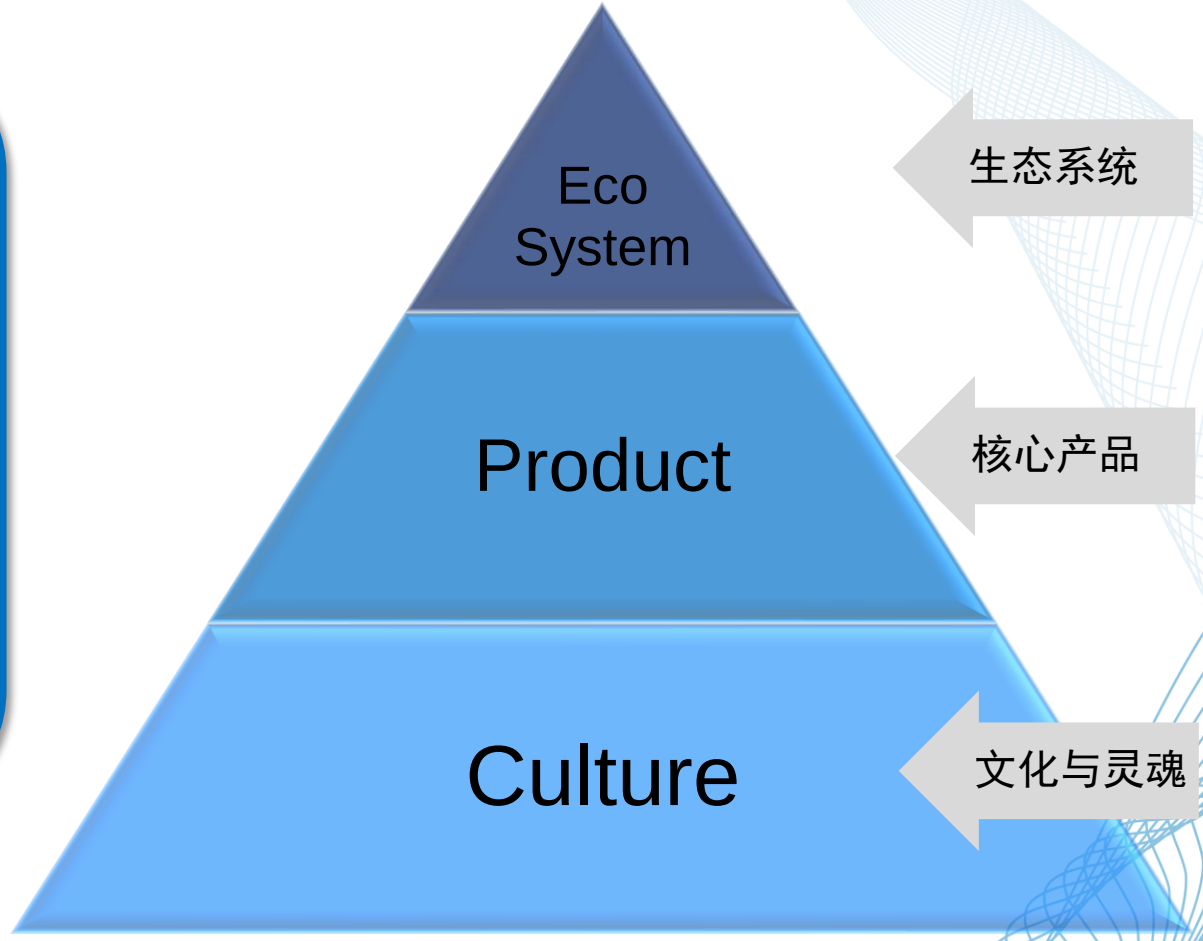
Benefits of our Certifications
QNX安全认证的优势

- **可互换的软件**
  - 安全认证操作系统和虚拟机监控器(QNX Safety-Certified OS and Hypervisor)与同类QNX产品100%兼容，并且具有良好的互操作性。
  - 安全和非安全版本使用相同的平台代码，共享API和文档。
- **高质量**
  - 评估由TÜV莱茵（TÜV Rheinland）进行，TÜV莱茵是知名且备受尊重的审计专家。
  - 大多数认证的评估范围包括x86及32位和64位ARM架构的运行时和开发工具。
- **强大的安全文化**
  - QNX拥有完善的功能安全和网络安全文化，具有专业正规的系统开发流程。
  - QNX在获取认证方面具有100%的成功率。

QNX Safety and Security Value Proposition
QNX功能安全与网络安全的价值主张

QNX为功能安全和网络安全系统提供强大、可靠平台的承诺：

- 行业领先的安全认证
- 高质量、高安全性的软件
- 以安全为先的设计理念
- 长期支持的承诺
- 开发全面的生态系统



Thank you