立足伟大传统的前沿：铁路安全软件

火车是真正意义上最古老的机械交通方式。作为第一种不依赖人力或天气的交通工具，火车改变了我们生活和工作方式。从第一批蒸汽机车开始穿行于世界各地到如今已有两个世纪了，但火车依然处于技术、创新和安全的前沿。

地铁和轻轨每天要运送上千万的乘客。6,000 hp（4,500 瓦）机车可以拖动相当于100辆汽车的货运列车，总吨位要大于一艘海军驱逐舰。高速货车，例如法国的邮政高速列车，时速可以达到250 km，而像中国高铁这样的客运列车时速可到350 km。上海磁悬浮列车以430 kmh的惊人速度运行，而其最高可达时速为500 km！

这些列车必须依赖软件控制系统来实现启停、调整和保持速度，并在拐弯和受风力影响时保持平衡，确保沿着轨道行驶。软件控制系统最重要的任务就是保证乘客和货物的安全。

安全传统

火车拥有悠久的安全传统和在安全方面的创新，因而它依然是最安全的交通方式之一。

二十年前，欧洲电工标准化委员会的EN 50126、EN 50128 和 EN 50129 成为首批从宽泛的IEC 61508中衍生出的细分行业标准，这并非偶然。而IEC 61508则是电气/电子/可编程电子安全系统的功能安全标准。铁路从业者不仅清楚安全的重要性以及安全运行铁路系统的条件，而且在200年间立足于技术创新的前沿，寻求在功能、效率和安全之间实现最佳的且可行的平衡。

当今的列车包含了众多嵌入式软件系统以实现各种功能，从调整每一个机车车轴上的扭矩和滑移，到通信信号收发和驾驶室仪表操作等等。列车不仅仅是机车和车厢；还包括了庞大的轨道网络、交叉点、车站、调车场等等。所有这些都必须工作到位，才能保证列车准时准点且安全地运行。

QNX 和铁路

实时操作系统（RTOS）几乎是每个安全软件系统的核心所在，而QNX在这一领域积累了三十多年的经验—对软件而言，这几乎相当于钻木取火的历史之长— 而QNX系统对列车安全和效率的支持几乎也有同样长的历史。

欧洲隧道列车模拟装置

为了实现商业可行性，连接英格兰和欧洲大陆的欧洲隧道每日需要通行1200次列车。而问题是，在1994年欧洲隧道开通前，没有几个列车工程师能够以160公里的时速驾驭列车通过50公里的海底隧道。

在隧道开通前，负责培训第一批英吉利海峡隧道列车司机的法国公司EBIM为欧洲之星、C92和Le Shuttle列车提供了基于QNX技术的模拟装置。这是全球首批具备完整驾驶室环境的动态铁路模拟装置，针对巴黎-伦敦-布鲁塞尔这一完整线路提供三轴移动、完整声效和车站间电脑成像。

GE Evolution 系列机车

GE Evolution系列机车赋予了柴油机车新的含义。这些庞然大物能产生4,400 hp（3,300瓦）的马力，其中每个轴上的1,000 hp逆变器可以调整扭矩和滑移，而它们要用至少20个基于QNX平台的奔腾系统来维持机车运行、沿轨行驶和节能高效。这些系统要衡量和检测的参数多达5,000个，而数据延迟根据每单一功能的需求，从几十微秒到几十秒不等。

GE Evolution系列机车在美国设计制造，如今它们驰骋于五大洲来往运送货物。2009年，哈萨克斯坦国家铁路获得第3,000台该系列机车，而在中国，6,000 hp（4,500 瓦）定制款GE Evolution系列机车不久将运行，同当前用于中国主干线的列车引擎相比，它们可以多产生75%的动力，而排放的氧化亚氮（NOx）要减少28%。

Xworks 列车通信系统

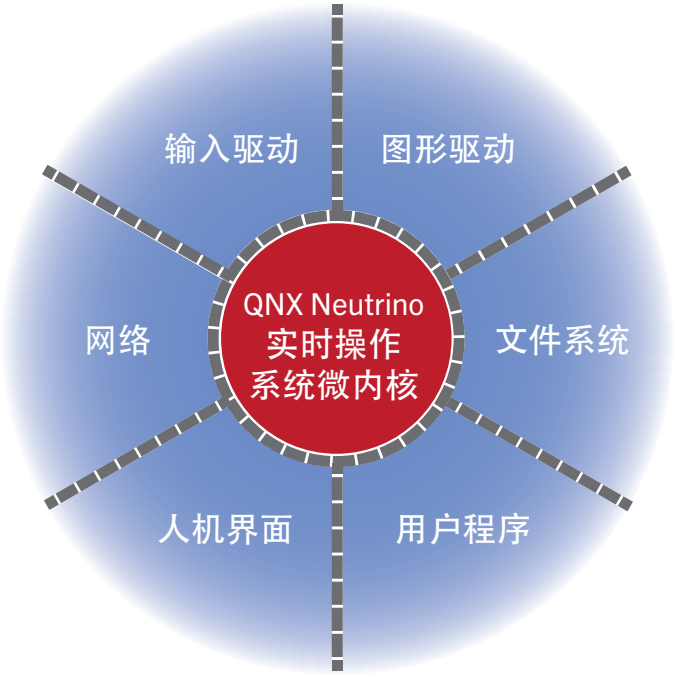
ONTRACK是一个负责新西兰铁路网的政府组织，通过运行一个覆盖全国的无线电系统，来支持列车安全运行，协助轨道工人的工作。ONTRACK最近升级了这个涵盖148个山顶和隧道特高频中继器的系统，使用Xwork通信系统，结合用于列车和山顶通讯的特高频模拟无线电，以及在QNX Neutrino实时操作系统上运行的RoIP网。

Xworks是一个四频道的RoIP装置，也被称为ORC，能够增强可靠性、灵活性和对移动数据的支持。它连接了传统的VHF/UHF无线电网络和IP网络。操作者可以在新西兰国家列车控制中心远程管理和控制这一全集成、低带宽且厂商中立的RoIP解决方案。

技术领先

显然，200年中一切都已改变。蒸汽让位于柴油和电力。通信员和他们的通讯标志以被现代技术补充和取代，例如列车自动保护装置（ATP）和精确列车控制（PTC）等。自Salamanca在英格兰运行起的两个世纪中，铁路运营的成功取决于技术的创新。从机车设计到轨道钢材，所有一切都发挥着作用，直到今天依然如此。

对领先技术的需求在控制列车和轨道网络的软件要求中渐渐显现。由于操作系统是所有软件系统的基础，所以系统的技术创新和整体成功归根结底有赖于操作系统。无论是用来管理机车发动机和油耗，保证安全车间距，还是收发信号进行通信，管理复杂驾驶室系统，从可靠性出发，这些操作系统就必须始终满足一系列的关键要求。



独特的QNX微内核实时操作系统架构可以防止一个零部件的故障对其他程序或内核产生破坏作用这种情况的发生。该实时操作系统可以自动进入安全状态，或重启任一故障零部件。

实时可靠性

安全的软件系统也是可靠的软件系统：它可以同时满足可得性和可靠性的相关要求。它必须在要求反应时有所反应（可用性），并且其反应必须是准确的（可靠性）。

例如，控制列车制动器的软件系统必须在所需之时做出反应— 反应延迟可能会引发事故，同时它的反应必须可靠：制动器的应用必须恰到好处— 制动太弱可能会引起碰撞，而制动过强可能会损坏列车，致使乘客受伤或引发脱轨事故。简言之，过长的反应时间或不恰当的回应都可能导致悲剧发生。这种可得性和可靠性的实现需要实时的性能。因此，适用于这些系统的唯一选择便是实时操作系统（RTOS），它可以满足可靠性和可用性的不同需求。

认证和国际市场

全球的铁路逐渐转向列车自动保护装置（ATP）和精确列车控制（PTC）等相似系统以确保安全性。北美、欧洲和其他地方的政府都开始要求这些系统通过

认证过程漫长、艰难且昂贵，但也是上市前至关重要的一个环节。即便不是明文规定，这些认证也能提供显著的竞争优势，这是因为它们是不可争议的第三方证词，来证明该系统符合相关的安全要求。

例如，采用一个通过IEC 61508 安全完整性三级认证（SIL 3）的实时操作系统，并且与了解该认证的流程的供应商合作— 从管理开发环境到验证可靠性— 可以大大减少成本，降低安全软件系统开发过程中固有的风险。

QNX安全内核

QNX® Neutrino® 实时操作系统安全内核已通过IEC 61508 SIL3认证。在其提供的认证平台上，应用程序开发者可以运行相关系统，而这些系统必须满足最严格的功能安全要求。

开发工具

出色的开发工具能够提供软件开发项目的关键优势：它们可以帮助开发者深入了解系统并调整其性能，减少开发、调试和验证的时间和精力。这不仅能转化为更有效率、更安全的系统，而且能大量节省用于开发、审批和认证的时间和费用。

性能、连接性和人机界面

用于列车控制软件系统内的实时操作系统必须运行迅速，且具可预见性。它也必须提供中间件设施，用以支持列车不同零部件之间，以及与列车系统信号系统间天衣无缝的通迅。最后，只要铁路系统中有人工操作员的存在，那么操作系统必须支持人机界面（HMI），这些界面则必须易于使用、明确且直观。

QNX Neutrino 实时操作系统

早在现代技术盛行之前，铁路从业者就明白技术优势是成功的基石。

QNX Neutrino 实时操作系统每月在单核和多核系统上的运行时间数以千万计，是用于嵌入式计算的首屈一指的实时操作系统，无愧于任何铁路安全关键型软件系统的重要组成部分。