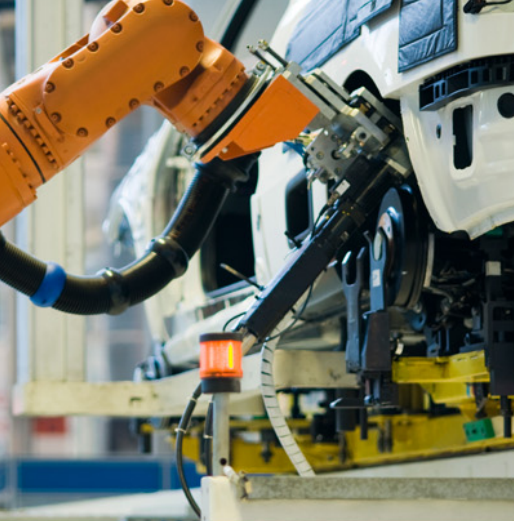




工自市场技术探讨
功能安全以及实时协定

工自市场产品经理 郑怡

2012 年 QNX 中国技术创新会议



无所不在的工业自动化



潮流与挑战

- 硬件的发展
 - 处理器速度提高, 功能增加, 支持的附件更多
 - 生产商亟欲合并硬件以减低成本
- 软件的发展
 - 设计复杂性提高, 软件行数增加, 更易出错
 - 全自产软件可能性日小
- 企业发展需求
 - 有效节省开支
 - 应对审核压力
- 技术要求
 - 实时性能
 - 可靠性和可用性
 - 认证过关



功能安全之亮点

- 对功能安全的要求在诸多工自市场中越来越重要，个中原因包括：
 - 技术性原因：系统设计越复杂，故障的几率也越高
 - 诉讼风险：事故所能导致的赔偿超过预防措施的费用
 - 政府部门和监管团体的积极介入
- 为不同市场量身定制的功能安全标准也如雨后春笋般出现
 - IEC 61508: 功能安全的“元老”标准
 - IEC 62304: 医疗器械
 - ISO 26262: 车载系统
 - ISO 61311: 工自流程
 - 还有更多层出不穷...



功能安全定义，众说纷纭

- 功能安全的技术定义十分明确：“执行某种功能” + “提供安全保证”
- 然而不同的安全标准对功能安全有不同的定义
 - 有些标准明确设立一些详细规定
 - 例如，IEC 61508 强烈推荐使用正式设计方式来达到 SIL4
 - 有些标准则注重于需要达到的目标
 - 例如，ISO 26262 要求汽车生产商进行内部审核来证明自己能够达到某项 ASIL
 - 有些标准着眼于产品生命周期流程
 - 例如：IEC 62304 明确定义医用软件生命周期，但是对不同等级医疗设备的可接受故障率却只字不提
 - 有些标准有量化的达标准则
 - 例如：IEC 61508 明确定义，要达到 SIL3，产品的危险故障率必须在每小时 10^{-8} 到 10^{-7} 之间

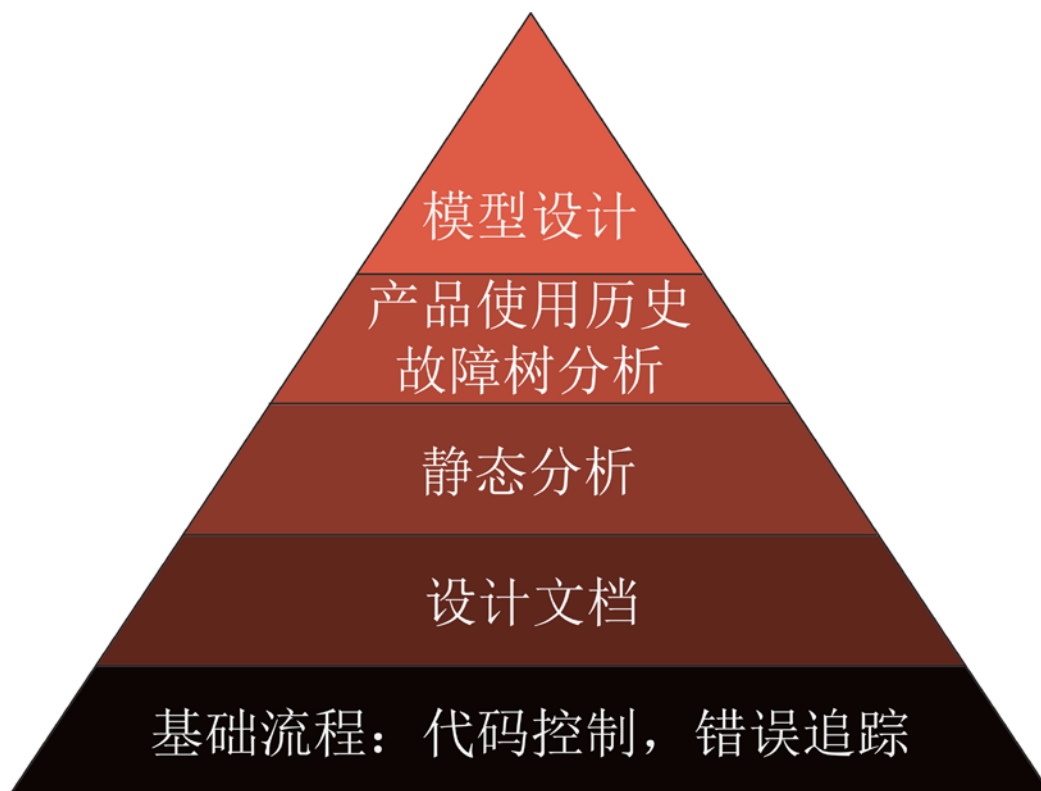
成功要诀之一：安全风尚

- 培养企业的安全风尚是保持长久优势的最佳策略，不仅能够有力说服认证机关，而且对于创造良好的市场形象也有帮助
- 很多功能安全标准都要求企业设立专门监管与安全相关事务的人员和部门
- 为企业内部培养功能安全领域的人才，积累着一方面的知识和经验，提供培训是一条捷径
- 真正意义上的安全风尚远远不止于维持一个安全产品的生命周期，而是体现在每个员工对功能安全的认知和重视上
- 安全风尚的真伪很难混淆，建立安全风尚是一个长期的任务，公司高层的认可和支​​持是必不可少的。



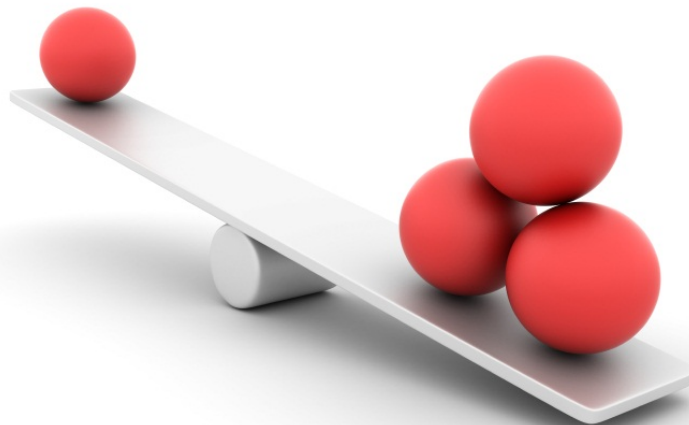
成功要诀之二：了解认证过程

- 产品认证是一个冗长而且昂贵的过程，成功率并非百分之百
- 认证员也是凡人，也有不同的风格，他们对于一种标准可能会有不同的诠释



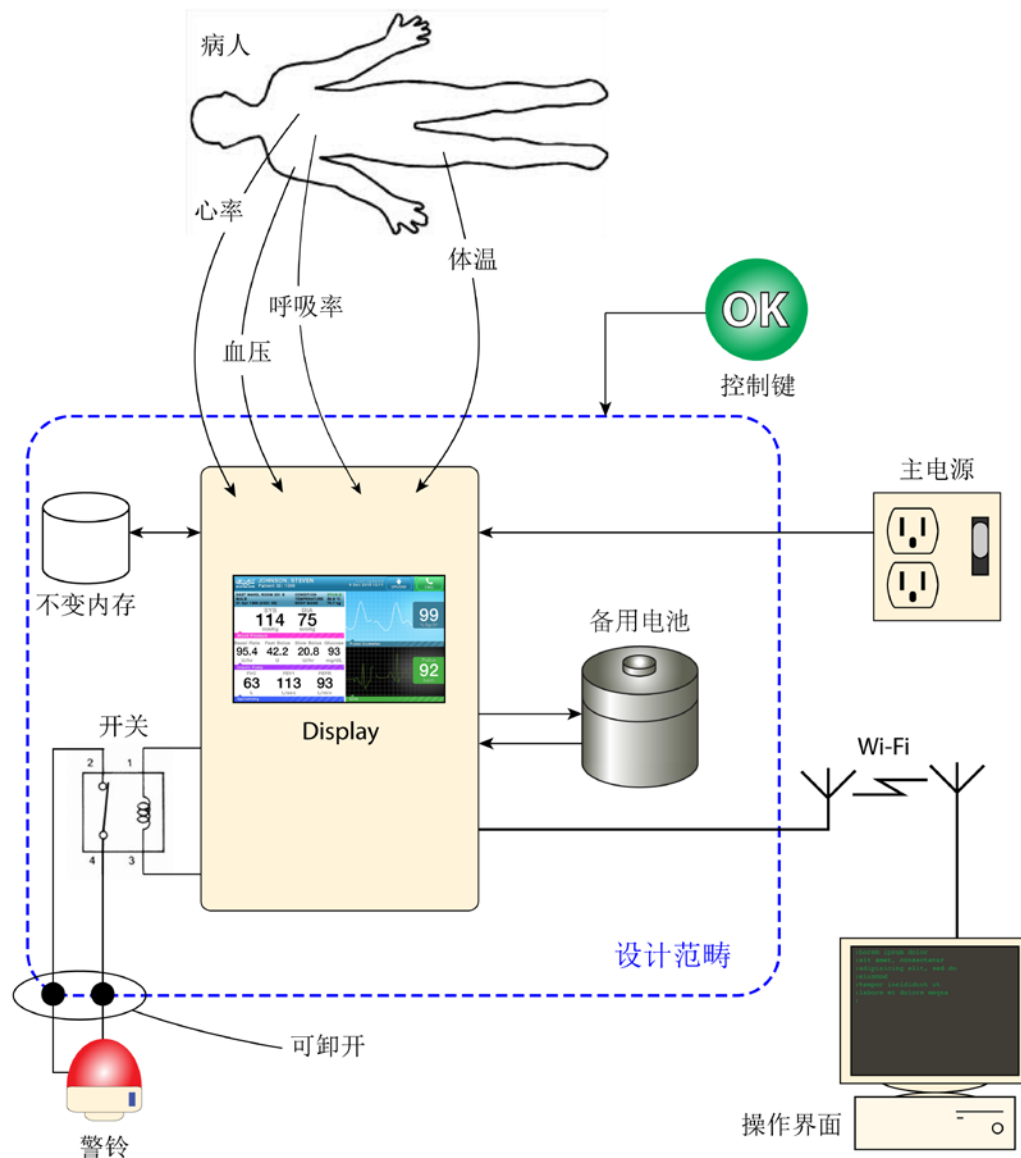
成功要诀之三： 巧用外力

- 设计功能安全产品并通过认证并非易事，所以应该尽量借用外力和资源
 - 采用先进的工具，设计方案和流程，例如
 - 静态分析工具
 - 正式设计方法
 - 设计证明
 - 采用已通过认证的组件
 - 和有认证经验的供应商紧密合作
 - 接近有认证资格的团体
 - ISO 团体(可加入社交媒体)
 - 认证公司



医疗实例

- 为显示正式设计方法的潜力和用途，QNX 设计了这个以患者检测器为题的演示
- 采用的正式设计工具是来自欧联盟的免费工具“罗丹”，所用的设计语言叫做 Event-B
- “罗丹”中的设计是循环式的，从港开始十分简单原始的设计，逐步增加要求，增加变量，定量和命题，渐渐达到无懈可击的设计
- “罗丹”中的设计证明功能成功地为我们指出了原先遗漏的设计要求，及早防止了错误设计的发生
- 虽然实现这个设计的工程师是一位资深功能安全设计人员，但是这个工具还是捕捉到了人力无法捕捉的错误！

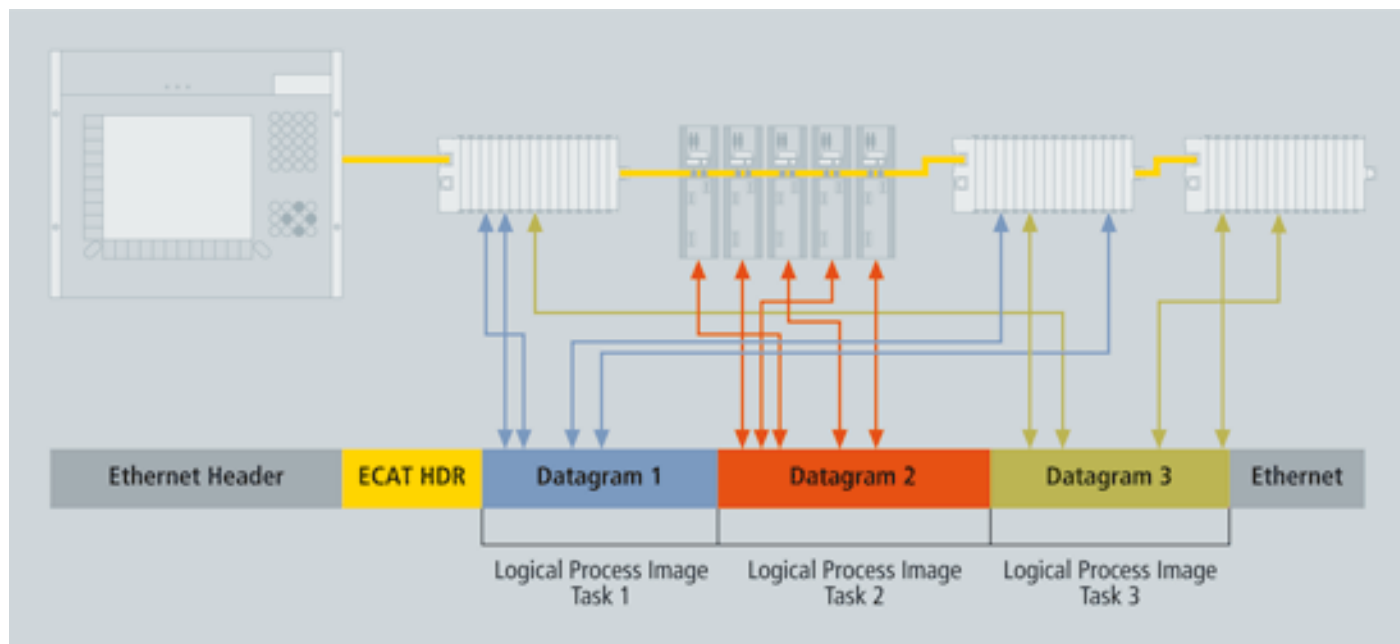


工业协定入门

- 常见名称
 - Common Industrial Protocol (CIP): 通用工业协定
 - Open DeviceNet Vendors Association (ODVA): 开放 DeviceNet 厂商协会
- 常用协定
 - Ethernet/IP (北美比较流行, 主要用户包括洛克威尔公司)
 - EtherCAT (全球性协定, 其采用越来越广泛)
 - PROFINET (欧洲比较流行, 主要用户包括西门公司)
- 普遍特性
 - 实时性能
 - 很多协定都是开放式的
 - 比较新的工业协定一般都基于 Ethernet, 很多都依赖 TCP/IP
 - “从零开始”自己编写协定的厂家很少, 一般都使用现有解决方案

细看 EtherCAT

- 名副其实：Ethernet for Control Automation Technology
- 三大设计目标：信息更新时间短，通讯抖动小，硬件成本低
- 由德国倍福公司（Beckhoff Automation）研发的开源式协定
- 秘诀：不需要看的不看！



技术简介

- 硬件
 - 从站控制器
 - 从以太网帧中读取和从站设备相关的数据，并在报文中插入输入数据
 - 通过 FPGA 实现（如德州科技新推出的 AM 355 系列）
 - 主站
 - 标准以太网 MAC 卡或标准网卡已经绰绰有余
 - 由于一两个以太网帧已经即可完成与所有段子的通讯循环，所以协定对主站的 CPU 几乎没有什么消耗
- 软件
 - 系统配置工具软件
- 拓扑结构：总线形，树形或星形
- 性能
 - 数据量：一个以太网帧可以交换 1486 字节
 - 带宽利用率：从 4.8% 到 90% 以上

EtherCAT 和 QNX

- 协同工业协定合作伙伴 König
 - König 为 EtherCAT 提供成熟的解决方案
 - 主站和从站协定
 - 系统配置和诊断工具
 - 在多种硬件平台上支持 QNX: x86, Power, ARM
- 实现真正的实时

Cycle Times in μ s							
Required	50	100	50	100	50	100	1000
Average	49	109	49	99	50	99	~980
Jitter	-1	9	-1	-1	0	-1	~-20
Minimum	43	104	39	86	42	89	~400
Maximum	57	123	59	113	57	111	~10000

Yi Zheng
yzheng@qnx.com

© 2012 QNX Software Systems Limited. QNX, QNX CAR, NEUTRINO, MOMENTICS, AVIAGE and other product names are or may be registered trademarks and/or trademarks of QNX Software Systems Limited (QSSL) or its licensors in Canada, the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of QSSL as of the date of this presentation. Because QSS must respond to changing market conditions, it should not be interpreted to be a commitment on the part of QSSL, and QSSL cannot guarantee the accuracy of any information provided after the date of this presentation. QSSL MAKES NO WARRANTIES, REPRESENTATIONS OR CONDITIONS EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

