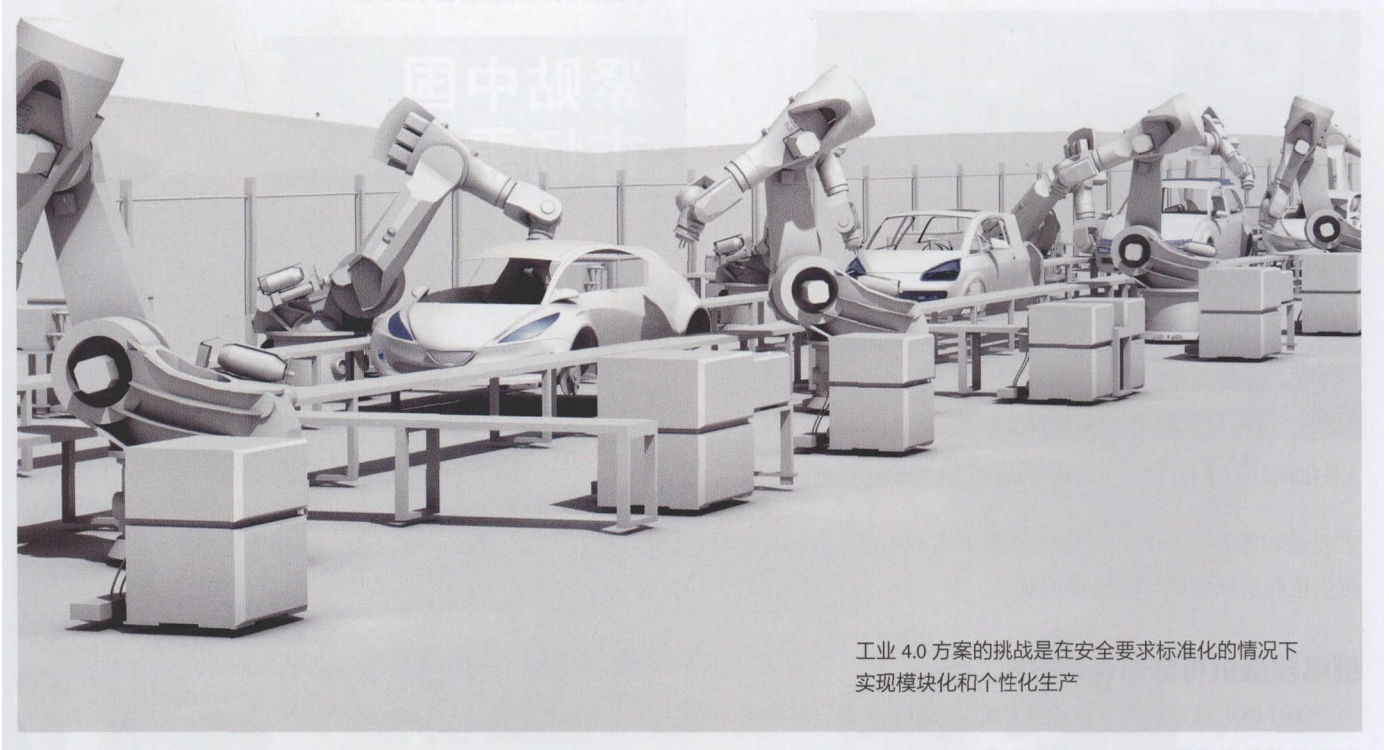




工业 4.0 方案的挑战是在安全要求标准化的情况下实现模块化和个性化生产

工业 4.0

工业 4.0 和功能安全

为了落实工业 4.0 这一未来项目，还必须解决一些技术上的难题，机器设备的灵活性和模块化以及在多种协议的基础上联网都需要功能安全性方面的全新解决方案。

文 | Steffen Horn



工业 4.0 这一未来项目包括产品价值创造链的各个阶段和领域，很长一段时间以来，企业、协会、大学、媒体甚至包括联邦政府都在跨界讨论第四次产业革命，但这一模式并不仅仅涉及生产地德国，其他工业国也以“工业互联网”（美国）、“未来产业”（法国）和“产业价值链倡议”（日本）等名称将自动化和 IT 融合起来，中国也尝试通过与德国或美国合作的方式介入这一主题。各种集团都在定义结构模型以便理解这一主题，同时将其作为对自动化系统研发人员的指导和帮助，不管这些结构模型有

什么名称，是 Rami4.0（工业 4.0 的参考架构）还是 IIRA（工业互联网参考架构），它们都在描述相同的技术发展及其机会和风险。

针对工业 4.0 的问题多于答案

无论从哪个角度来看待这一未来项目，工业 4.0 都同样建立在一些原则和常量的基础上：不论是有前途的商业模式、个性化的产品、订制和制造过程、小批次、数字化、联网、云计算、所有与互联网有关的产品、机器和设备的灵活性和模块化。所有参

与部分的共同点在于，一台机器或设备可能对人类和环境造成的风险必须低于社会能够接受的风险，第四次产业革命也不会改变“功能安全性”这一原则。

作为功能安全性自动化和通信技术的供应商以及解决方案的提供者，菲尼克斯电气非常清楚自己的责任，这是由国家法律，如机械条例以及 IEC 61508 等国际标准来落实的，模块化机器和设备的灵活性以及不断增加的安全相关组件的联网带来了新的挑战，如今问题多于答案。

多达 31 个安全岛的横向通信

通过安全桥技术的系统步骤 V3 可以在一个安全桥岛内最多集成 16 个不同的安全 I/O 模块, 这些模块单独安装, 并根据要求集成至标准数据网 (图 1)。

这样就可以处理最多 256 个安全输入口, 此外 V3 版本可以实现最多 31 个安全桥岛的相互通信, 这对模块化机器和设备的实施特别重要。

因为这样就可以安全地连接和分开机器部件。

对于安全桥 V3 而言, 标准现场总线系统 Profibus、CAN、Devicenet 和 Interbus 以及工业以太网系统 Profinet、以太网 / IP、Sercos III、Modbus TCP 和 Ethercat 都可以共享。

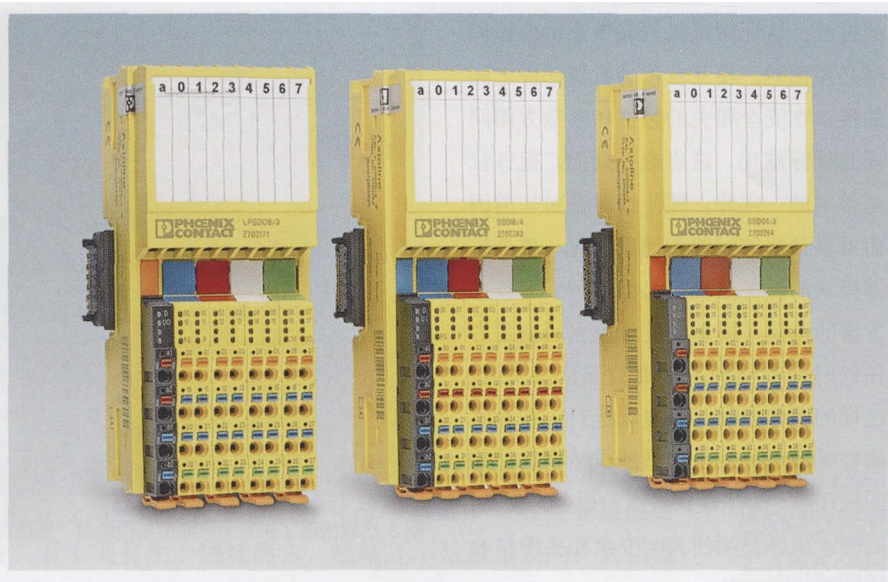


图 1 安全桥技术如今已在支持模块化、跨网络 and 安全的工业 4.0 通信原则

灵活的模块化设备

对一台机器进行安全设计时, 符合规定的第一步操作是确定边界, 这点乍一看与灵活、智能、自我配置和升级的

模块化机器相互矛盾, 而这些都是工业 4.0 这一未来项目所要求的。

即使考虑到这种矛盾还没有消除, 研发者和设计者都面临着一个雄心勃勃

胡默尔连接器系统 (上海) 有限公司——德国胡默尔集团的全资子公司, 于1999年在上海成立, 专业生产电缆接线技术中所需的各种旋紧件、铠装电缆接头、接插件、软管及配件、工业控制箱、自动化元器件等。

胡默尔公司的产品秉承德国传统的精湛工艺, 拥有多项专利技术和专业认证, 优异的品质已在全世界得到公认。



hummel
www.hummel.com

胡默尔连接器系统 (上海) 有限公司

市场销售部: 上海市黄陂北路227号中区广场1701室 (200003)

电话: +86-21-63758551 传真: +86-21-63758553

E-mail: info.hcs.cn@hummel-group.com

广告

的挑战，认证测试机构和专业协会也同样必须面对。相互合作的机器部件之间的接口在安全相关的数据和参数方面同样必须标准化，这点毫无疑问，但这只是答案的一部分，即使针对提前知道因而可以预测的配置和动态变化，单个机器模块的开关过程也必须进行安全技术方面的监控（图 2），比如整台设备是否任何时间都能满足必要的安全相关值，这样的监控当然应该自动进行，企业不需要采取额外的组织措施或承担复杂的配置任务，为了做到这点，适合工业 4.0 的安全组件必须使其与安全相关的核心价值能够动态读取。

模块化设备的认证过程同样必须简化，根据机器部件自我配置的观点，模块化设备的“可预见性使用”有着完全不同的意义，测试和认证机构面临新的任务，只有同组件制造商一起才能完成这些任务。

上述实例表明，怎样通过针对灵活性的技术方法鉴定和评估功能安全方面的新危害和风险，必须制定适当的错误识别技术措施，努力控制风险。此外互联网所有事物之间日益强大的全球通信会在数据安全交换方面产生以前没有见过的全新模式。

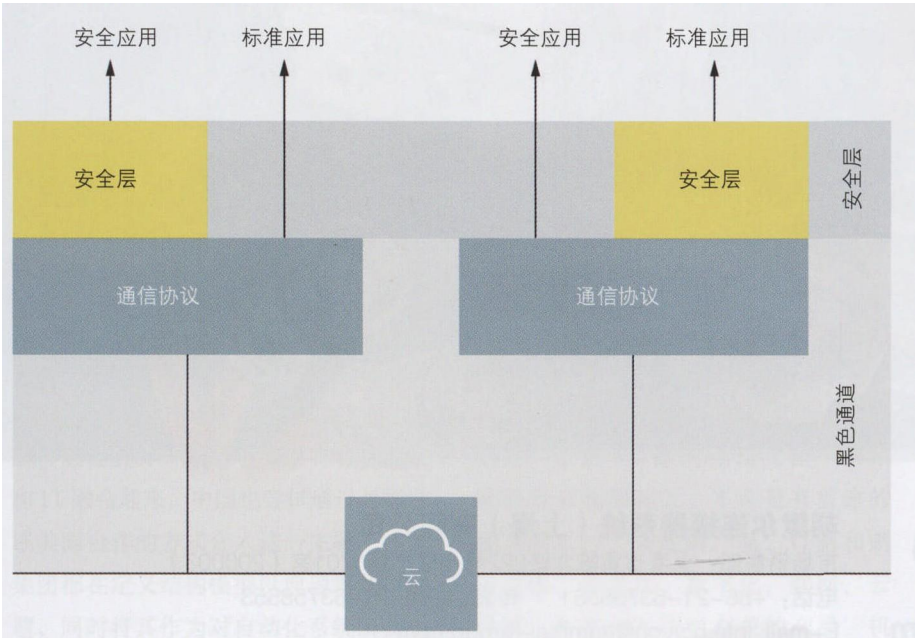


图 2 在智能工厂模型设备 OWL 中，单个设备模块的开关过程必须进行安全技术方面的监控



图 3 这就出现了未来无限通信是否遵循“黑色通道原理”这一问题

以“黑色通道原理”为基础

当前大部分 IEC 61784-3-3 国际标准安全传输协议都以所谓的“黑色通道原理”为基础（图 3），通信错误，比如出现在不安全的 IP 电报或基础结构组件中的，可以通过安全通信端点的错误识别措施以及足够的残余错误概率探测出来。根据 IEC，黑色通道原理的前提条件是所用标准基础设施和传输介质的精确定义以及在封闭界限内假设的错误率，根据对各标准通信协议的分析，人们会对识别错误的技术措施进行详细说明。

与控制系统有一定关系的不同标准

数据协议的差异反映出来，这使来自不同生产商的、使用其他控制系统和安全通信介质的设备之间的安全数据交换十分困难，唯一的解决方法是目前使用的安全网关，这会产生相应的硬件和配置开支。

机械生产商同样不愿意放弃这些优势，它们能够带来以互联网为基础的全球通信和云服务，这里也需要落实安全功能，作为“无限”传输安全相关数据和参数的解决方法，保护所有未知通信路径和互联网基础设施组件并不合适。分析了新的错误模式之后，安全协议的保护措施及其安全通信端点应当进一步完善，这类举措包括针对全球可靠鉴定的新方法或通过自我动态修改的完整安全回路对安全报文进行自动运行时间控制。

容易操作的方案很有必要

模块化机器的灵活性和全球联网的实例展示了功能安全领域的挑战，认证机构检测了所有解决方案中错误识别措施的效率，他们必须在机器和设备生产商的研发和设计办公室里证明其技术的可行性，只有做到了简单易行，最终用户才会接受这些方案。

“简单就是安全”这一座右铭是菲尼克斯电气公司安全组件、安全系统和安全解决方案的基础，这在工业 4.0 时代愈发重要。MM