工业物联网在半导体行业中的机遇

作者

Ron Lowman
战略营销经理
Synopsys, Inc

序言

据 Fortune Business Insights 预测，2018 年，工业自动化市场规模为 1570.4 亿美元，到 2026 年，这一数字将超过 2967 亿美元，年复合增长率达到 8.4%1。这一增长势头将直接影响拥有先进人工智能 (AI) 能力、更高安全性和可靠性、强大连接能力、更高吞吐量和防护能力的新型半导体设计。

工业半导体的设计目的是对多项应用进行控制，包括工艺控制、工厂自动化、机器人、太阳能逆变器、计量、资产跟踪、能量收集、监控摄像头、医疗、3D 打印机、航空电子设备等。

根据维基百科的定义，“第四次工业革命 2（或者叫工业 4.0）是采用现代智能技术对传统制造和工业实践进行持续的自动化。大规模机器对机器通信 (M2M) 和物联网 (IoT) 集成在一起，从而实现更高自动化程度，更好的通信和自我监控，以及生产能够在无需人工干预的情况下分析和诊断问题的智能机器 。”

多家全球市场领导企业正在推动工业 4.0 的实施。国土安全研究公司提供的名单中有多个半导体领导者和系统集成商，包括霍尼韦尔、NEC，三菱电机、SAP、高　通、Rockwell Automation、3D Systems、Alphabet、Dassault Systems、Advantech、IBM、Denso、思科、博世、西门子、Thyssenkrupp、谷歌、三星、惠普、德州仪器 (TI)、ABB、华为、通用电气、英特尔、甲骨文、Kuka、微软和 Beijer Electronics。

其他公司还包括 Preferred Networks、OMRON、Parker-Hannifin、Yokogawa Electric、Emerson、Fanuc、Schneider Electric、Tyco、UTC、Mitsubishi 等。

图 1 显示了帮助推动工业 4.0 的半导体技术。

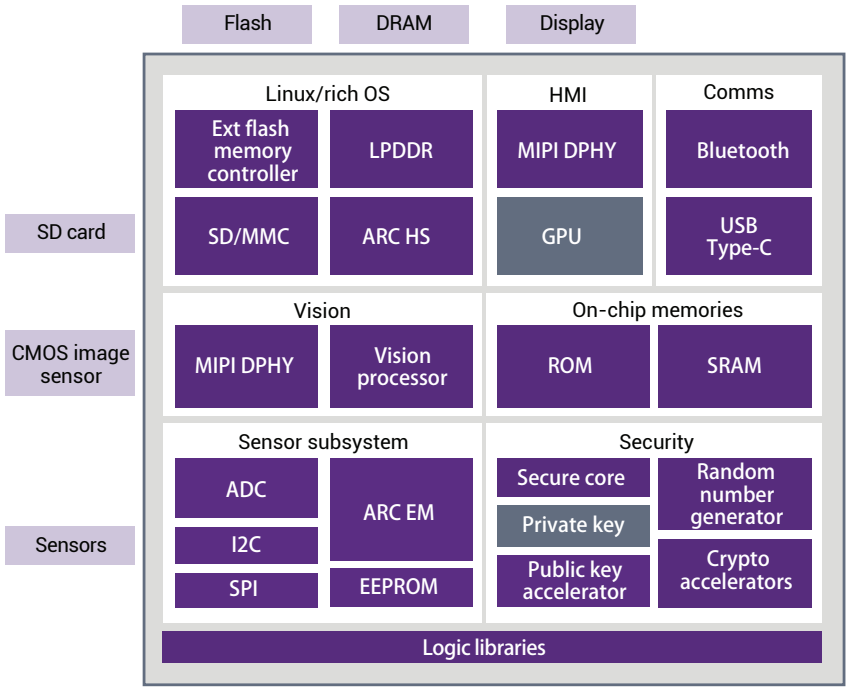

图 1：通用工业 SoC 框图示例

如图 1 所示，据半导体行业协会 (SIA)3 的数据表明，工业半导体约占全球半导体市场总量的 12%。一些公开报道显示，工业物联网 / 自动化市场增长势头强劲，特别是在中国。

根据法兰克福国际机器人联合会 4 的数据，中国的工业机器人产业是增长最快的市场，增速高达 21%。报道显示，到 2021 年，中国当前 800 多家机器人制造商将使中国工业机器人出货量占到全部市场的 45%。根据 Axa Insurance5 的数据，2020 年，中国的新基建计划将通过物联网连接超过 2000 亿硬件设备，其中 95% 以上由中国制造。

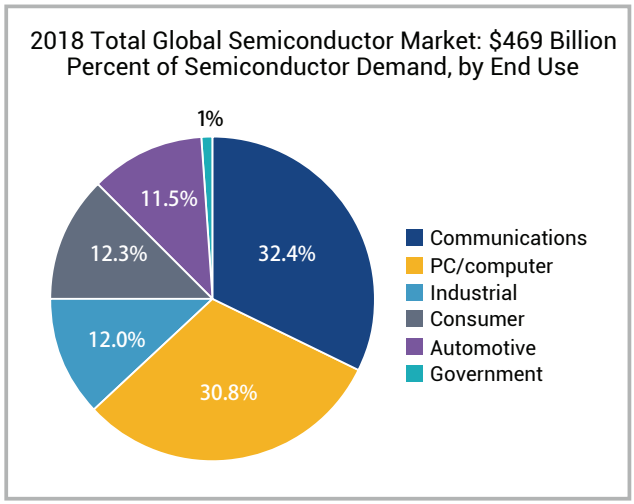

图 2：按最终用途划分的半导体需求百分比（图片由 SIA 提供）

半导体行业的主要工业趋势

针对工业物联网的半导体设计的增长受到 AI 集成、安全性和可靠性、连接能力、吞吐量和防护能力等多种趋势的推动。

AI 集成

毫无疑问，AI 推动着自动化和运营效率的显著提高。这方面的例子包括缺陷识别、库存管理、预测性维护和可视计数能力。这些 AI 能力需要嵌入到工业半导体和系统中的专用处理器，提供大量的乘积累加运算，以确保处理时间和能源消耗不高于设计目标。

安全性与可靠性

工业制造控制要求采取严格的可靠性和安全预防措施。IEC 61508 规定了不同的安全完整性等级 (SIL)。工业应用领域的半导体通常需要在多个不同用例中遵守安全标准，包括工艺自动化、机械、铁路、核能等，如图 3 所示。半导体厂商、半导体供应商甚至 IP 供应商都可能要遵守许多文档记录、可靠性和设计活动，使系统集成商通过 IEC 61508 子类别认证。这些活动对于确保安全和可靠性措施的制定和不断改进至关重要。

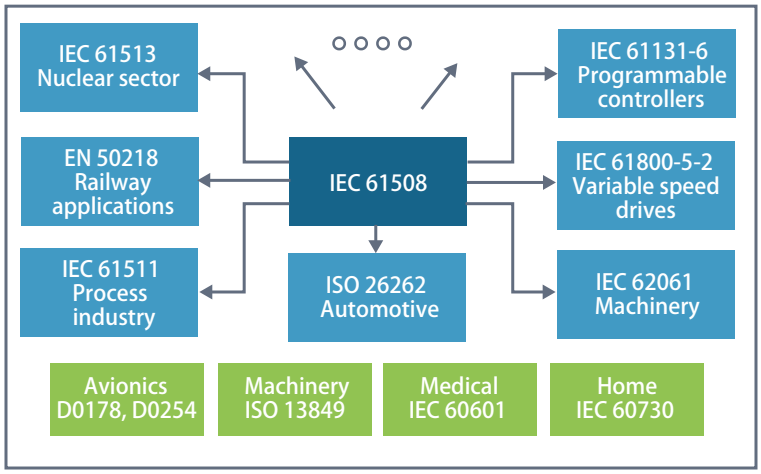

图 3：多个不同用例中的安全标准

连接能力

工业 4.0 要求工厂车间和公司 IT 部门形成一个整体。这需要聚合多种不同的通信协议。多年来，工厂一直面临着为提高效率而投入高昂成本升级专有和旧版本通信协议的困扰，而 IT 部门在管理不断变化的消费者技术方面疲于应对。许多通信协议增加了软件抽象层，旨在更好地向互连程度最高的工厂转型，包括 CoAP、MQTT、XML、HTTP、AMQP 等。基础硬件技术也在迅速演变，以提供低延迟、带时间戳且功能丰富的兼容性连接能力。

吞吐量

许多工业系统需要通过更高的带宽而提高工厂效率。数十年来，工业系统一直通过从串行协议转变到以太网协议而实现持续改进。无线技术也正在工业系统中得到快速采用。然而，底层的半导体 IP 协议在系统改进方面也发挥了重要作用。这包括更高内存吞吐量、在工业系统增加更多 SoC，以及具有高可靠性的长距离以太网能力。

防护能力

全球互连带来了新的风险。互联网连接相关的勒索软件、IP 盗窃和其他恶意活动对安全防护提出了明确的需求。保护制造和商业基础设施中的宝贵资源已成为工业设计的重要考量因素。有些领域还有其他标准和最低安全要求。半导体和支持系统越来越接受通过硬件安全方法正确实施和维护这些升级。

主要挑战和 IP 解决方案

人工智能（例如机器视觉）需要采用专门的处理器减少功耗，缩短计算时间，同时需要可靠、强大的传感器连接能力。这需要多个关键 IP 组件。这些系统的传感器接口采用最新的 CMOS 图像传感器，而这些传感器变得越来越复杂，包括多种图像数据格式、高级颜色、高分辨率、SNR 等。

MIPI CSI-2 IP 解决方案满足了机器视觉的基本连接需求，包括每通道最高 4.5Gbps 的速度和 24 位精度。最近，这些解决方案新增了智能关注区域能力，可以仅在需要时才传输数据，这一能力非常适合机器视觉。新思科技推出了全面的 DesignWare MIPI IP 产品组合，包括 CSI-2、DSI/DSI-2、D-PHY、C-PHY 和 I3C，可确保设计人员采用可靠的连接解决方案进行工业实施。

视觉处理器也是针对 AI 算法的高效处理能力而优化的关键组件，包括标量、矢量和神经网络数学的异构计算能力，以及在可实现的芯片面积内支持此类复杂系统的基本软件基础架构。用于嵌入式视觉解决方案的新思科技 DesignWare ARC EV 处理器从一开始就是专为采用优化型卷积神经网络（CNN）和递归神经网络（DNN）引擎的机器视觉应用而设计。DesignWare EV7x 视觉处理器的性能高达 35 TOPS，可为机器视觉提供最先进的深度学习处理能力。

工业 SoC 的可靠性和安全性考量一直是整体系统要求中的重要组成部分。然而，许多工业应用都很难找到合适的半导体解决方案，因为大多数工业应用的体量不能保证定制硅片的合理性，鉴于此，系统集成商不得不自己构建，或者依靠传统半导体供应商修改或升级那些无法满足严格可靠性和安全性需求的现成解决方案。但当前，新思科技提供的 IP 拥有满足行业应用所需要的许多安全性和可靠性文档、流程与特性，使系统集成商或半导体提供商更容易采用满足安全性和可靠性需求的关键 IP 模块构建 SoC。DesignWare ARC 处理器和接口 IP 解决方案（如 PCI Express (PCIe)、DDR、MIPI、USB 和其他许多 IP 解决方案）提供了必要的流程、文档以及可靠性和安全性方面的特性，可满足非常严格的工业安全要求。这包括存储器中的错误检查校正 (ECC) 能力、文档以及为保障安全性和可靠性而提供的固有流程。另外，用于启动时进行冗余检查的双锁步处理和安全管理器、定期测试管理以及用于安全机制测试的错误注入等 IP 特性满足了功能安全方面的全部需求。

强大的连接能力要求工业半导体同时使用有线和无线 IP。近年来，对以太网时间敏感网络 (TSN) 功能的支持需求一直提高。新思科技推出了支持 TSN 的以太网控制器，已在工业应用中被广泛采用。基于 802.15.4 的解决方案为计量、工厂自动化和楼宇控制提供了连接能力，但最近，随着 Google、Amazon 和 Apple 等大型提供商为利用基于 802.15.4 并整合低功耗蓝牙、Thread 和 Zigbee 确保无缝互连的解决方案实现家庭自动化提供了路线图，互操作性不断成熟。新思科技的 DesignWare 蓝牙、Thread 和 Zigbee IP 凭借优化的功耗、性能和面积 (PPA) 为此类硬件实施提供了基本的构件。

更高的系统吞吐量还使工业系统能够以低延迟能力实现实时控制。几十年来，许多工业系统的响应时间都无法实现远程实时响应，而实施的项目仅限于批处理或远程监视。随着 5G 的出现及其将响应时间降低到 1ms 以下的目标，工业市场中的新应用成为了探索的目标。随着半导体 IP 的发展，例如支持高达 400G 和 800G 以太网的高速 SerDes PHY，实时工厂控制和其他应用成为可能。DDR5 和 LPDDR5 等存储器接口增加了系统的内存带宽和容量。目前，PCIe 5.0 也被迅速采用，用于连接工业服务器以及芯片到芯片的高速接口。特别需要指出的是，Compute Express Link (CXL) 协议专注于提供低延迟和缓存一致性能力，可为系统设计提供更大的灵活性，并缩短工业服务器和网络接口卡（NIC）的响应时间。新思科技是接口 IP 领域的领导者，为工业 SoC 设计提供了最全面的经过硅验证的 IP 解决方案。

安全破坏事件越来越多，而且我们需要实施硬件来保护系统免受这些威胁的侵害。为了防御这些攻击，硬件的信任 IP 根至关重要，包括在引导和 SoC 运行期间的保护。现在，为加密数据的传输而加速实施协议安全的举措越来越多。保护工业 SoC 所需的 IP 包括真实随机数生成器 (TRNG)、安全引导、安全区域 (Secure Enclaves) 和受信任的执行环境、安全协议加速器等。新思科技推出了全面的安全 IP 和软件解决方案。最近，接口 IP 协议的发展正加速安全硬件的采用。

领先的工业企业都已在其工业 SoC 中采用了新思科技的 DesignWare IP。通常，工业物联网 / 自动化 SoC 设计正在取代传统的 FPGA 和现成的解决方案，因为这些解决方案无法满足快速增长且差异化的工业物联网需求。新思科技 DesignWare Security IP 已经满足安全引导、密钥管理、安全调试和安全固件更新等工业需求。公司在 IP 和实施方面的专业知识已经满足工业 SoC 的严格要求，并且其表现优于内部、现成和 FPGA 解决方案。

总结

未来工业半导体市场提供的机遇会持续增加。相关企业需要通过迁移而采用更多定制解决方案，以满足快速变化的虚拟世界中对 AI 能力、安全性和可靠性、连接能力、吞吐量和防护能力等方面的需求。工业应用的半导体 SoC 需要借助 IP 解决快速变化的环境所面临的关键问题。这些问题包括高效的计算、可靠的通信以及安全的数据交换。要实施下一代解决方案，像新思科技这样拥有经过硅验证的 IP 解决方案组合的合作伙伴非常重要。

参考资料

1. https://www.fortunebusinessinsights.com/industry-reports/industrial-automation-market-101589
2. https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution
3. https://www.semiconductors.org/wp-content/uploads/2019/05/2019-SIA-Factbook-FINAL.pdf
4. https://www.cnbc.com/2020/03/02/the-rush-to-deploy-robots-in-china-amid-the-coronavirus-outbreak.html
5. https://www.axa.com/en/magazine/internet-of-things-made-in-china

09/17/20.CS558031567 SG Industrial IoT Opps in Semicond WP.

发布日期：2020 年 9 月