到2027年，您还“安全”吗？

新欧盟机械法规

对机器和移动机器人的影响

新欧盟机械法规促使移动机器制造商采取行动

欧盟机械指令

2006版欧盟机械指令（指令2006/42/EC）是欧盟各国国家产品安全法的一部分。因此，所有在欧盟市场销售或进入欧盟市场的机械产品都必须符合该指令的要求。

指令中规定的要求是 CE 标志的基础，CE 标志向用户证明机器在投放市场时在机械和电气方面是安全的。制造商申请CE认证的前提条件是必须提供符合性声明，同时还需要执行全面风险分析。

机械制造商可以按照关于控制系统安全相关部件的多种协调标准（《机械指令》中明确应用的标准，如关于机械安全的 ISO 12100 和 ISO 13849-1）准备符合性声明。因此这些标准是支持遵守《机械指令》的重要手段。

历经数月，经过多次讨论、协商和修改，最终版新《欧盟机械指令》终于在2023年6月29日正式发布（见图1）。今后该指令将更名为《机械法规》，名称为“法规（EU）2023/1230”。经过42个月的过渡期后，该新法规将于2027年1月14日前强制实施。届时，所有想在欧盟制造、销售或经营机械产品的企业或个人都需要遵守该法规。
需要注意的是，过渡期结束后，所有欧盟成员国需要以相同方式将新《机械法规》作为一项法律进行实施，即必须强制遵守。

“机械”一词的定义非常宽泛，从单个设备或单独执行某种功能的组件，到由多个机械设备构成的装置，都属于机械范畴。因此，CE 认证所需的工作以及确保机械安全所需的程序和机构也大不相同。虽然关于单个设备符合性声明的风险评估流程在可控范围之内，但系统集成商要想获得CE认证，需要考虑更广泛的风险因素。特别是，机器部件之间的接口以及与用户之间的接口在功能安全和信息技术安全方面都提出了新的挑战；《机械法规》现在明确规定要应对这些挑战。

除了修订了设备和装置清单外，其中一些（如移动机器人）是首次被明确提及，新文件还考虑到了反映机械行业最新技术水平的新技术和新工艺。特别是基于软件的安全功能、自学习安全系统，以及大量机械性能监控和记录功能，如内置诊断和日志记录功能。

截至撰写本文时，关于协调标准清单以及IT安全标准交叉引用的问题仍未解决。目前，后者仍处于不断变化之中；《机械法规》标准委员会尚未决定是否直接引用IEC 62443、IEC 27100和欧盟《网络弹性法案》等安全标准从而实现这些标准的协调统一。

从另一方面来看，这意味着进一步修改完善《机械法规》是不可避免的，因此在该法规正式生效前，这些不足之处还可以得到弥补。

《机械法规》从63页增加到了102页，这本身就表明过去17年技术发展突飞猛进，需要对旧版指令进行修订。下面通过几个示例重点讲述制造商、集成商或最终用户可能或将要面临的挑战。

以移动机器（AGV和AMR）为例说明机器更改要求

更改机器的“实体”将变为“制造商”

旧版《机械指令》中未明确规定且经常引起争论的事项称为“重要更改”。什么更改视为“重要更改”？这种更改对整个系统的CE合规性有何影响？

新《机械法规》对“重要更改”给出了更清晰的定义，将其描述为可能会导致新危险情况或加剧现有危险的任何更改（无论是电气还是机械方面）。

任何此类更改都会影响整个系统的CE合规性。因此，更改机器的实体在法律上成为机器制造商。因此，该实体必须满足《机械法规》中的相关要求。

以移动机器人系统为例进行说明：

目前，实现移动机器人系统之间的互操作性已成为一个明显的趋势。欧洲VDA 5050和美国MassRobotics等统一通信标准的制定就是一个明显的标志。

对最终用户来说在一个系统中操作不同类型的机器人或机器人类型，乍一看似乎非常方便。用户购买新机器人后，可以使用标准通信接口将其集成到现有系统中，从此不再依赖各个制造商和集成商。

但他们很快就会发现，添加一种新机器（例如，在以前只使用单元货载系统AGV的地方添加自动叉车），甚至安装一种新软件组件以进行远程维护，都可能会导致新危险情况。虽然制造商出售的各台机器会将其视为固有安全且符合CE标准，但这不一定适用于因集成机器而被修改的整个系统。

在集成新类型的机械之前，至少需要重新执行风险分析。如果分析结果表明这会给整个系统带来新危险或加剧现有危险，那么最终用户将成为整个系统的制造商，并有义务满足《机械法规》的相关要求。在这种情况下，对现有系统进行更改前，先委托独立专家（TÜV、VDI等）进行初步评估会很有帮助。

图1：适用于欧洲移动机器人制造商的安全标准

监控功能：远程安全停止移动机器

未来与自主移动机器制造商相关的一项特定要求是《机械法规》附录III 第 3.2.4节中描述的监控功能。

移动机器必须允许管理人员远程接收与该机器有关的信息。这些信息应能使管理人员全面、准确地了解机器在行驶和工作区域中的操作、移动和安全定位情况。

此外，还应使管理人员能够安全停止和重启机器，或者将机器移到没有危险的安全位置（见图2）。

实现这一点的关键是能够通过无线网络传输安全相关信号，因为移动机器通常不直接通过有线通信技术传输信息，以免移动受到限制。要传输此安全相关数据，并遵守《机械法规》相关要求及基于该法规的标准（如ISO 3691-4），建议使用PROFIsafe或CIP Safety等现场总线安全协议。尽管这些协议最初并不是为无线传输而设计，但由于它们都基于黑色通道原理而构建，因此原则上也可以用于无线传输。不过，由于架构不同，有些协议在无线网络中存在明显的性能差异。如需详细了解各个协议及其用于无线网络时的优缺点，请参阅相关HMS白皮书（https://www.ixxat.com/safety-protocols-go-wireless）。

所有这些协议的共同点是确保无线网络稳定，这对整个系统正常工作至关重要。因此，在设计网络和要传输的数据时，必须考虑避免干扰，并尽可能减少数据传输量—需要多少就传输多少。否则，对于由数百台移动机器组成的机器群，如果无法将各条安全消息可靠地传输给预期接收者，很快就会出问题。为了应对通信不可靠问题，系统必须能够自行切换到安全模式。通常情况下，这意味着能够安全关闭系统或至少能够安全关闭系统中的某些部分。在这种情况下，不稳定的无线连接会导致严重的停机。

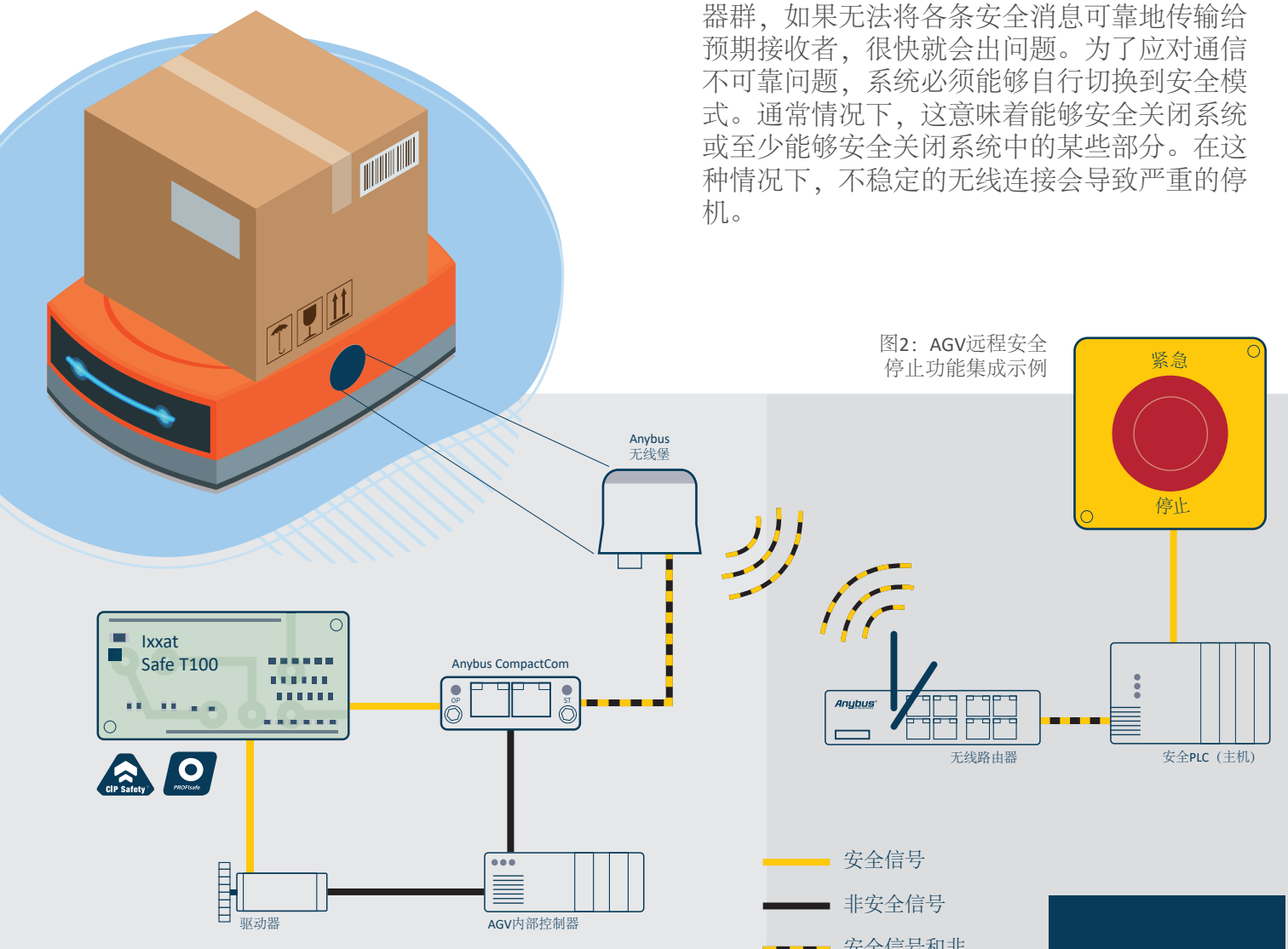

图2：AGV远程安全停止功能集成示例

移动机器和系统制造商面临的另一个挑战是分开两个不同的安全电路还是将它们合并为一个电路，其中，一个是“慢速”外部安全电路（例如，上述监控功能采用的电路），该电路容忍长达数百毫秒的周期时间；另一个是车辆上的“快速”安全电路（例如，行人探测系统采用的电路），对于该电路，需要在极其危险的情况下做出实时反应。此示例说明，机器制造商和系统集成商需要密切合作，以在实践中正确实施《机械法规》要求的功能。

防篡改：系统安全与日志记录要求

无论是过去还是现在，对现行《机械指令》进行修订都主要是出于IT安全考虑。

虽然过去通常将功能安全和IT安全分开考虑，但随着机器之间及机器与全局网络之间的互联程度越来越高，这两个领域现在的融合度也越来越高（见图3）。广泛地讲，功能安全是指保护人员免受机器伤害，而IT安全则是指保护机器免受人为破坏。

早在2010年，Stuxnet蠕虫病毒恶意篡改工业设施可能导致的危险就引起了全球关注。几乎每天都有关于公司和设施遭受网络攻击的最新报道。

因此，在新《机械法规》中将这一点纳入考虑是当务之急。未来，仅在机器和互联网之间设置防火墙将再也不能满足需求。

即将实施的新《机械法规》在附录III中的“防止损坏”部分对此进行了详述。系统制造商必须确保连接笔记本电脑等第三方设备不会导致危险情况。而且，机器在未来必须能够识别和收集有关合法及非法干预安全相关组件（包括软件组件）的信息。

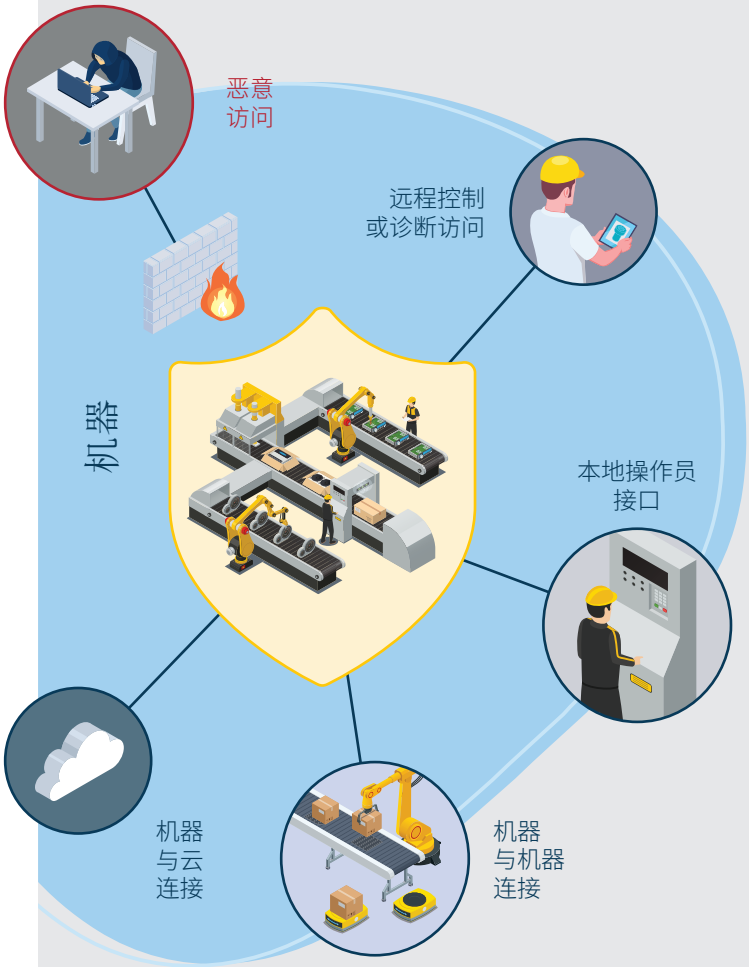

图3：特别需要确保机器接口的功能安全和IT安全

总结：机器制造商面临什么挑战？

前面通过列举示例描述了机器制造商在努力遵守欧盟法律要求时将会面临的一些挑战。保护人员、财产和环境免受机器的危害仍然是首要目标。

欧盟对现行《机械指令》进行了重大修改，尤其是安全方面，这方面的法律要求将会更加严格。未来，机器需要能够识别和记录攻击信息，并尽可能防止遭受攻击。制造商应尽早考虑这些问题，并与经验丰富的合作伙伴合作，共同寻找解决方案以达到新法规要求。

新法规将移动机器明确纳入进来的目的是制定明确的机器相关要求，消除当前可能会引发误解和歧义的“灰色地带”。

到2027年新《机械法规》生效之时，将不可避免地增加关于协调标准的引用内容，弥补当前标准化工作中存在的不足。这意味着，如果想在2027年后成功将此类产品推向欧盟市场，所有制造商就必须在开发新产品时富有远见。

标准将继续为制造商遵守《机械法规》提供重要支持，而使用预先认证的组件将能简化系统设计。