Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland/Germany
www.pilz.com

背景资料

2026年7月

自动化网络中的“区域与通道”：信息安全保障机械安全

安全是重中之重

奥斯菲尔登，2026年7月 –

《机械法规》对此作出了强制性规定：工业信息安全旨在保护与安全相关的功能免受篡改 -

换言之，信息安全是安全功能正常运作的前提。但如何为自动化网络提供全面保护呢？IEC 62443-3-2等标准以及即将发布的EN 50742标准都指明了明确的方向：将系统划分为不同区域，并对连接进行监控 -

这一原则贯穿于行业机构和专家当前提出的各项建议之中。Pilz坚信：将安全与所谓的标准自动化严格分离，是实现有效机械安全的关键 -

这一理念以“深度防御”原则为基础，并通过“区域与通道”方法加以实施。

一栋房屋可以建立得坚固安全：墙体结实、采用防火材料、电气系统可靠，并配备能正常工作的报警装置。这种结构安全是机械安全的一个典型范例，其中设计措施、传感器技术和防护机制旨在预防意外危险。然而，只有在没有受到人为干扰的情况下，这样的房屋才能保持安全。被篡改的供暖控制系统、遭破坏的电路或被关闭的报警系统，

都可能使一座原本以安全为设计宗旨的建筑变成一个隐患。在机械领域，如果未经授权擅自篡改或禁用与安全相关的部件，即使是最完善的安全相关设计也会失效。

在此背景下，信息安全发挥着外部防护的作用：坚固的门、安全的出入口、受监控的连接以及防止未经授权干预的屏障。因此，信息安全并非旨在防范事故本身，而是防止保护机制被禁用 - 例如，防止有人通过选择未经授权的操作模式或采取未经授权的操作来获取访问权限。只有这样，安全才能始终可靠地发挥作用 - 以信息安全保障机械安全。

从监管要求到解决方案建议

《机械法规》（EU）2023/1230首次将安全性确立为工厂和机械正常运行的强制性要求：安全功能不得因任何形式的篡改（无论是否故意）而受到损害。这正是新出台的EN 50742标准发挥作用之处；它将有助于阐明《机械法规》中的基本信息安全要求。该标准规定了防止数据损坏的技术细则，并对可能影响安全功能的硬件、软件和数据提出了明确的要求。该标准涵盖了整个生命周期 - 从开发到运行再到退役。现有的IEC 62443系列标准为工业自动化系统和控制系统制定了系统化的网络安全方法，也发挥着关键角色。它为风险分析、“深度防御”以及分区原则（

“区域与通道”）提供了一个结构化的框架，并在EN 50742标准中被明确认可为保障信息安全的一种替代性或补充性方法。这些标准共同构成了“安全保障”的规范核心：它们要求将机器的数字完整性视为其功能安全的前提条件，并予以相应保护。

为什么 “区域和管道” 能让机械更安全

回到房屋这一比喻意象：锅炉房代表一个区域，而与智能家居网关的连接则代表与之对应的传输通道。如果该连接遭到篡改，整个系统都可能受到影响——即使该房间的安全措施再完善。因此，不仅要确保各区域的安全，还要保障连接这些区域的路线的安全。这正是“区域与通道”原则发挥作用之处。各区域之间界限分明，且区域之间的过渡地带均设有监控设施。就像在房子里，门和配发的钥匙决定了谁能去哪里一样，工业厂房内部的防护（机械安全）与防止外部篡改的防护（信息安全）在结构上是相互交织的。

由此形成了一种基于“深度防御”原则的防护理念：安全性并非通过单一防护措施来实现，而是通过层层递进的多重防护措施来实现的。如果攻破了一层防线，下一层依然坚如磐石。这些分层空间由“区域”构成，而“通道”则是连接它们的受监控通道。这样一来，单个漏洞就不会危及整个系统 - 尤其是当这关系到安全问题，进而关系到人员安全时。

Pilz始终贯彻“信息安全保障机械安全”的理念，其中“安全”是“安全保障”的首要保护目标。重点在于保障安全，从而保护人员安全。正因如此，Pilz将安全功能与一般的机器控制（即标准自动化）分离，从而降低了安全相关功能的风险。这些“资产”在功能上划分得越明确，为提供可靠保护所需的额外安全措施就越少。

这种方法的优势在机器的整个生命周期中都显而易见。如果安全功能与标准功能是分开的，那么当标准功能进行更新时，无需对安全功能进行并行重新认证或调整。这大大减少了维护和保养工作。传统的安全控制器所需的安全关键型更新也远少于标准控制器，因此这种分离消除了许多不必要的干预。分离式设计还具有技术优势：像PNOZmulti 2这种独立的安全控制器，可以自由地与不同厂商的控制系统进行组合，而集成式系统往往受限于特定技术。与此同时，独立的安全解决方案提高了攻击者的门槛，因为必须分别攻破各个独立系统，这使得操控变得困难得多。此外，标准系统可在需要时保持在线状态，而实际的安全功能则保持隔离，从而大幅缩小了攻击面。

将安全自动化与安防自动化进行分离 -

两者各自拥有完美协调的信息安全级别——

还能通过简化安全、维护和扩容措施的规划工作，从而提高效率。因此，对标准程序的更改无需对安全相关部分进行任何干预，从而大大减少了所需的编程和调整工作量。同时性，这种分离对软件和支持成本也产生了积极影响，因为独立的系统通常产生的许可证费和服务费较低。

分离保障安全 – 培训提升能力

将安全系统与标准自动化系统明确分离，不仅确保了系统的技术可靠性，还能减少操作员失误并降低培训要求。由于安全功能在专用硬件上运行，且在组织架构上与非安全功能明确分离，因此即使对标准程序进行更改，这些功能仍能得到保护。因此，日常运营中的失误不会影响安全，且职责划分也能更加明确。

Pilz提供全面的培训和服务方案，以帮助企业实施该架构。其中包括“工业信息安全基础”和“CESA – Certified Expert for Security in Automation”培训课程，以及工业信息安全服务。这些内容不仅阐述了如何基于各个模块构建稳健的“信息安全即机械安全”概念，而且远不止于此：它们展示了如何系统地管理安全风险并制定全面的安全方案，如何融入IEC

62443标准的要求，如何构建安全机器网络的架构，以及如何评估并持续改进所采取措施的有效性。

这种方法的一个关键优势在于：终端用户的操作人员无需深入钻研安全问题，因为安全功能的保护已由架构设计所保证。因此，这些培训课程主要面向负责安全决策或系统设计的人员 – 而操作人员无需接受工业信息安全方面的额外培训，即可继续安全地开展工作。其结果是实现了角色分工的合理化，这既简化了工厂的运营，同时又可持续地提高了防护水平。

清晰的架构与专业的技术，共同提升安全性

有效的“信息安全保障机械安全”战略并非通过单项措施来实现，而是通过周密设计的架构、明确的责任划分以及有针对性的技能培养来实现的。这正是Pilz大显身手之处。Pilz始终专注于“深度防御”，并明确区分安全系统与标准自动化系统，从而为打造具有韧性的机械设备奠定了基础 – 此外，我们还提供实操培训和咨询服务，确保企业能够充满信心地走上这条道路。其结果是，这种安全水平不仅符合标准要求，而且在日常运营中带来了切实的附加价值：操作更简便、更可靠，且长期来看更具成效。

((字数：9,640))

Pilz - 安全精神

Pilz是全球范围内的自动化技术产品、系统和服务供应商。作为安全自动化的先驱，Pilz为人、机器和环境创造安全。这家总部位于奥斯特菲尔德的家族企业成立于1948年，如今在全球拥有42家子公司和分支机构，员工人数达2500人。

该技术领导者为机械安全和工业信息安全提供完整的自动化解决方案。这些技术包括传感器、控制和驱动技术，以及工业通信、诊断和可视化系统。此外，还提供咨询、工程和培训等国际服务。除机械制造外，Pilz解决方案还应用于内部物流、包装、铁路技术或机器人等许多行业。

www.pilz.com

社交网络上的Pilz：

在我们的社交媒体渠道上，我们提供关于Pilz公司和其员工的背景资料以及最新的自动化技术消息。

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

新闻联系人：

Martin Kurth

公司与技术资讯
电话：+49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

技术与公司资讯
电话：+49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

技术新闻

电话：+49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

技术新闻

电话：+49 711 3409-7147
e.roessle@pilz.de