背景资料

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

2025 年 10 月

保护公司、机械和产品

机械安全和工业信息安全 – 一站式服务

2025 年 10 月，奥斯特菲尔德恩--**安全事件不再仅仅影响 IT 系统，而且越来越多地影响到生产环境 (OT)。工业信息安全事故不仅包括有针对性的攻击，还包括意外操纵。工业信息安全在生产中的使命是保证设备和机器的可用性，以及机器数据和流程的完整性和保密性。不过，最高保护目标仍然是功能安全。因为归根结底，如果公司对其数据没有主权，那么公司及其员工的安全就会受到威胁：没有安全就没有保障，而没有保障，人就得不到保护！**

欧盟内部已经认识到威胁日益加剧的形势，并对立法进行了相应的调整：**在公司**层面，**NIS 2 指令要求采取措施，例如通**过信息安全管理系统，确保欧盟内部具有较高的网络安全水平。

新的机械法规2023/1230

现在规定了设备和机械的防腐败措施，并要求对影响功能安全的机器部件采取安全措施。

网络弹性法案(CRA)要求对具有数字元件的产品采取信息安全措施。这些产品包括控制器、IO系统和机械中使用的其他组件。

公司、机械和产品 -

在各个层面，机械制造商和运营商都面临着不同的挑战和不同的法律框架。

先进的信息安全系统

除了立法者强制规定了必须要考虑工业信息安全，还有很多理由促使人们需要尽早处理这一问题并获得一些建议。如果不经常对机器操作的既定流程和条件进行质疑，就会助长操纵行为。例如，机器使用较长的一段时间后，其相应的系统往往会变得过时，在某些方面不再符合当前的安全标准。由于供应商停止提供安全更新，这些系统的安全漏洞已无法修复。有些设备，由于过于陈旧，无法在在终端设备上实施恶意软件防护，其性能也会因此受到影响，从而可能导致停产。

逐步提高工业信息安全

最终目的是确保业务运营始终受到保护，但要实现这一目标，企业必须克服各种挑战：从确定有效的法律要求、检测和修复系统中的漏洞，到提高员工的意识和培训，以及随后实施相应的控制措施。由于信息安全是一个不断变化的目标，因此有必要对机器设备的工业信息安

全状况进行常规检查。重要的是，公司内部要有明确的职责和系统的方法，包括积累必要的专业知识。

自动化公司PILZ皮尔磁已经为满足这些要求做好了准备，并为世界各地的机器制造商和用户开发了一套服务产品线，全面涵盖了人和机器防护的各个方面。PILZ皮尔磁的专家了解当前的法律和标准化要求，并将这些要求纳入他们的建议中。系统的培训让服务更加完善，使企业能够建立或更新其信息安全方面的知识。PILZ皮尔磁的产品解决方案有广泛的应用，例如身份识别和进入管理系统 - I.A.M.
系统，可以帮助用达到更高的机械安全和工业信息安全水平。

奠定正确的基础

为了确保机械设备的工业信息安全，机械工程专家需要具备扎实的基础知识，尤其是法规和适用标准方面的知识。我们的专家在“工业信息安全基础”培训课程中，会分享这些专业知识。学员将学习了解机械和网络安全方面的安全威胁、适当的保护措施和最佳实践。即使是安全领域的新手，也可以了解到可以采取哪些措施来有效保护机械免受网络攻击和机械生产层面的操纵。

"CESA - 自动化安全认证专家 "资格认证是PILZ皮尔磁提供的专家课程，为期两天，为学员提供符合最新标准的深入安全知识，尤其是 IEC 62443 系列标准（"工业通信网络 - 网络和系统的 IT

安全"）的相关内容。更重要的是，培训涵盖了实用的风险降低措施，如访问控制、利用技术手段提高网络安全性以及避免安全风险的组织措施。学员能够学习如何正确应用该标准，并证明其自动化系统符合网络安全要求。通过考试后，学员将获得由 TÜV NORD颁发的 "CESA - 自动化安全认证专家 "证书，该证书的含金量高，全球认可。

将理论付诸实践

在理论基础和培训的基础上，加强工业信息安全的下一步是应用结构化的实际流程。运营技术（OT）咨询是理论基础与可实施战略之间的桥梁。工业信息安全服务采用循序渐进的方法，识别复杂系统中的漏洞，并制定措施将风险降至最低。这就是一个整体的安全概念。

加强工业安全的四个步骤

运营技术的流程有四个步骤：保护需求分析、工业信息安全风险评估、工业信息安全概念和工业信息安全系统验证。

在保护要求分析的过程中，公司会确定工厂或机器中各个 "资产"的保护要求及目标。在第二步风险评估的过程中会对系统整个生命周期中每个分段的所有风险及其发生的可能性进行考虑。再下一步就是制定详细的工业安全概念，其中包括防御和降低攻击、操纵和操作失误造成的风险的战略和措施。此外，还为系统的持续安全运行或结构

制定了政策、规则和准则。最后一步是工业信息安全系统验证，检查已实施的应对措施是否有效。

确保机器可用性

工业安全服务流程有助于减轻或预防网络攻击，无意触发的安全事件也会减少。这反过来又提高了机器的可用性，最终确保节约成本，同时保持经济效益。

这种方法主要是利用适当的安全措施保护机器上的人员，因为安全事故可能会妨碍安全措施。例如，机器前的光幕可确保操作人员不会进入危险区域。但是，如果攻击者能够影响相关的控制器和机构，光幕的保护功能可能就无法保障。信息安全保障机械安全！

在机器的实际应用中，将机械安全和信息安全结合起来考虑是非常有意义的。因为：没有信息安全，就没有机械安全；没有机械安全，人就得不到保护！

明确控制：谁能在机器上做什么？

机器及其操作人员的安全取决于对人员或网络访问的控制。必须对入口点进行保护，防止未经授权的访问，例如，当机器正在运行时，任何人都不能进入危险区域。否则，即使是出于好意的设备操作或维护（无论是在现场还是通过网络）都可能造成致命的后果。

身份识别和访问管理（I.A.M.）是一项重要内容，它明确规定了公司内设备和机器的使用和访问权限，包括组织措施和规范，以及适当的机械安全和信息安全功能。PILZ皮尔磁的访问权限系统PITreader是一个合适的产品组件。它意味着用户可以达到员工保护、责任保护、最高生产效率和数据保护方面的要求。

我们坚信，只有采用全面的机械安全和信息安全方法，才能确保对人和机器的全面保护。是否以及在多大程度上处理安全问题，已不再是公司的自行决定，而是一项法律的要求。在工程设计中，工业信息安全方面的安全不再仅仅是IT部门的任务，而是设计和施工不可分割的一部分。因为，事后实施安全措施非常复杂，而且通常意味着用户友好性、功能和生产效率方面也有所折扣。

(字符：15，041))

((Box:))

欧盟工业信息安全立法概览

在欧洲，立法者针对威胁程度制定了一系列法律。因此，欧洲适应的法律有着非常严格的要求。其他国家的相关要求协议也已到位，将引入类似的法律要求。因此，工业信息安全的全球统一是可以预期的。

NIS2:公司的更多义务

NIS（网络与信息安全）是一项旨在加强网络安全的欧盟指令。该指令自2016年以来一直存在，目前适用于关键基础设施供应商，包括能源、交通、银行和金融、卫生、饮用水的供应和分配以及数字基础设施。这些领域的供应商必须实施“适当的信息安全保障措施”，并报告任何严重的网络安全事件。新的 NIS 2 指令（(EU) 2022/2555.....关于在欧盟范围内实现高水平共同网络安全的措施）要求今后有更多的公司采取网络安全风险管理措施。NIS 2将行业范围扩大到制造/生产行业，例如包括工程和电气设备制造商。其要求包括信息系统的风险分析和安全概念、供应链保护和人员安全。另一项要求是出入控制和设备管理概念，以及对管理人员的强制培训。

该指令于2022年底由欧洲议会和欧盟理事会通过。与所有欧盟指令一样，NIS 2在欧盟成员国不会立即生效并具有约束力，但欧盟成员国必须将其纳入国内法。公司最好尽快应对NIS 2，并对公司进行全面的安全评估。例如，这包括开发信息安全管理系统（ISMS）。在这种情况下，按照信息安全标准ISO 27001进行认证是有帮助的。

有了NIS

2，机器制造商，如发电设备（如风力涡轮机）的制造商，将来也必须满足这些要求。相对应的，风力涡轮机制造商也需要自动化解决方案、控制器或传感器。从一定规模来看，电气元件制造商也属于NIS 2的范畴。另外，由于NIS 2还规定要考虑供应商，像PILZ皮尔磁这样的公司也必须关注安全的供应链，并对其供应商提出要求。因此，NIS 2涵盖了整个供应链。

新的机械法规：没有信息安全，就没有CE标志

机械指令2006/42/EC在机械的功能安全方面具有特殊意义。

为了将机械设备进口到欧洲，机械制造商一直都必须通过相关的合格评估程序，并最终获得CE标志。

2023年6月作为机械法规重新发布，其规范已升级至最新技术水平。由于它是一项法规，因此不必首先将其转化为国家法律。机械制造商可在2027年1月20日前适应新要求，并从关键日期起满足这些要求。

《机械法规》取代了现有的《机械指令》，与前者相比，它使网络安全成为强制性的。如果说机械指令只是单纯地审查安全性，那么机械法规则将安全保护目标纳入“基本健康与安全要求

(EHSR)”，置于“防止腐败”之下：机械设备的安全功能绝不能因为事故或故意的腐败而有所妥协。

这一新的CE认证途径为机器制造商和运营商提出了许多新问题，因为他们需要修改现有的机械安全和信息安全理念。

网络弹性法案：整个产品生命周期的安全性

除了对公司和机器进行检查外，直接在设备（如控制器）中实施安全措施也是绝对必要的。2022年9月，欧盟委员会提交了一份旨在提高产品网络安全的法规草案。此网络弹性法案(CRA)面向具有数字元素(硬件和软件)且能够与其他产品通信的产品制造商。智能手机或机器人吸尘器等B2C领域的产品受此影响，控制器和传感器等B2B领域的产品以及操作系统或机器本身等纯软件产品也受此影响。

制造商对已利用漏洞的报告义务来自2026年11月09日。带有数字元件的产品必须从2027年11月12日满足CRA的要求，才能在欧盟市场上销售。CRA是一项欧盟法规，因此将在欧盟成员国立即生效。

CRA的影响究竟有多大取决于最终为产品分类制定的标准。根据CRA的规定，只有能够保证适当网络安全水平的产品才能投放市场，而且是在产品的整个生命周期内。因此，信息安全始于产品开发。这也是

多年来Pilz将其开发流程与IEC 62443-4-

1“工业自动化和控制系统的安全性 - 第4-1部分：

(字符：15，041))

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