

安全要求

打造全方位的安全

在一些特定的工业行业，行业操作者必须满足最低的安全要求，目的是防止对设备进行未经授权的操作。特别是在生产环境中许多企业都很少关心一些真实存在的潜在风险。因此一套完整的评估方案是很有必要的。



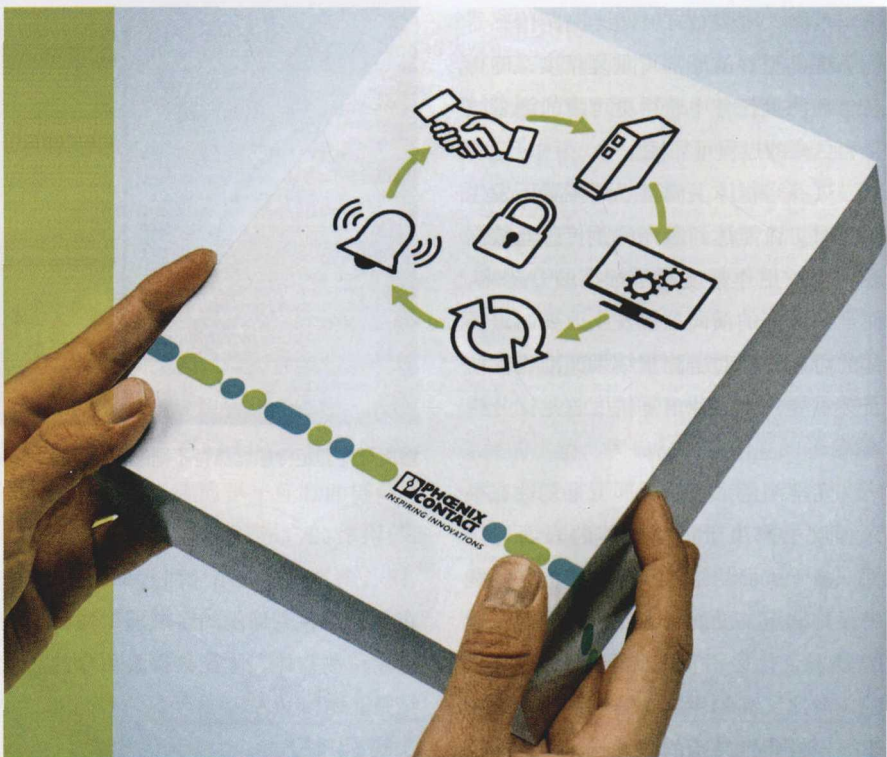
文 | Dr.-Ing Lutz Janicke

越来越多的企业致力于实现 IT 安全的构想。两大协会 VDMA（德国机械制造协会）和 ZVEI（电子技术工业中心协会）在众多行业内部进行的调查显示，目前执行率在中小型制造业还很低。据 ZVEI/BSI 研究表明，被调查的企业中仅仅只有 15% 的企业对其 IT 产品进行了风险分析。过去虽然报道了一些有名的事故——比如说“Wannacry”攻击，但是那些被“感知”到的危险情况现如今仍然没有得到足够重视。专家们一致认为，在工业 4.0 环境下电子化的增长和同期日益专业的计算机网络攻击加剧了危险系数。

在关键性的基础设施领域，立法者们结合德国 IT 安全法和欧盟 NIS 条例（网络和信息安全）制定了最低标准，从业者必须搭建一个由外部审计员确立的安全管理规则。关键性的基础设施领域包括了能源领域、信息技术和电信技术，健康、水、营养、交通运输、经济 and 保险业、国家管理机构以及媒体和文化业。

企业重视自身的安全问题

IT 安全包括了偶然的危险层面上的对信任度、数据以及系统的融合和可利



一直以来，去多企业真实存在的潜在危险都被过低评估了，即使其会带来巨大的危害。Phoenix Contact 可以利用他们的服务，产品和解决方案提供一个完整的评估

用性的保护，比如由洪水或火灾引起的，但是首当其冲的还是蓄意破坏。所以采取的应对措施也必须考虑到袭击者的犯罪动机。借由一套完善的评估可以达到这个目的。

最初的着手点是如何定义危险的企业数据。这不仅关乎到专业技术和程序数据，也关乎到特定系统的可利用性。对于那些一旦停摆就会带来严重后果的重要功能必须进行明确的强调。该任务

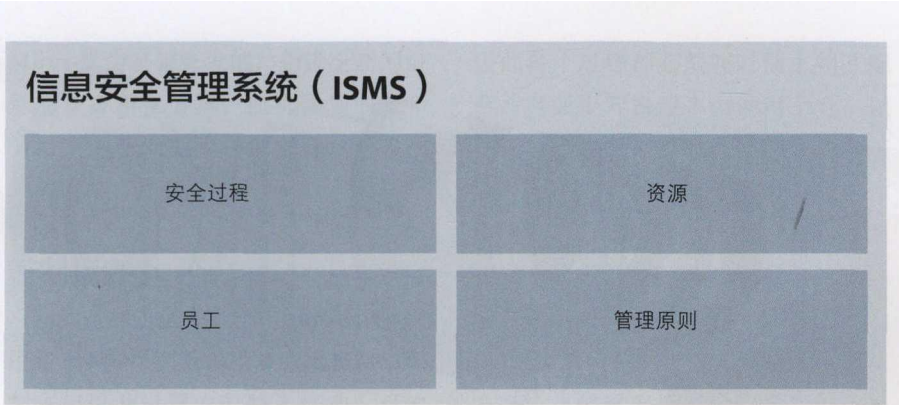


图 1 信息安全管理系统（依照联邦统计局关于信息技术安全统计）的四个组成要素

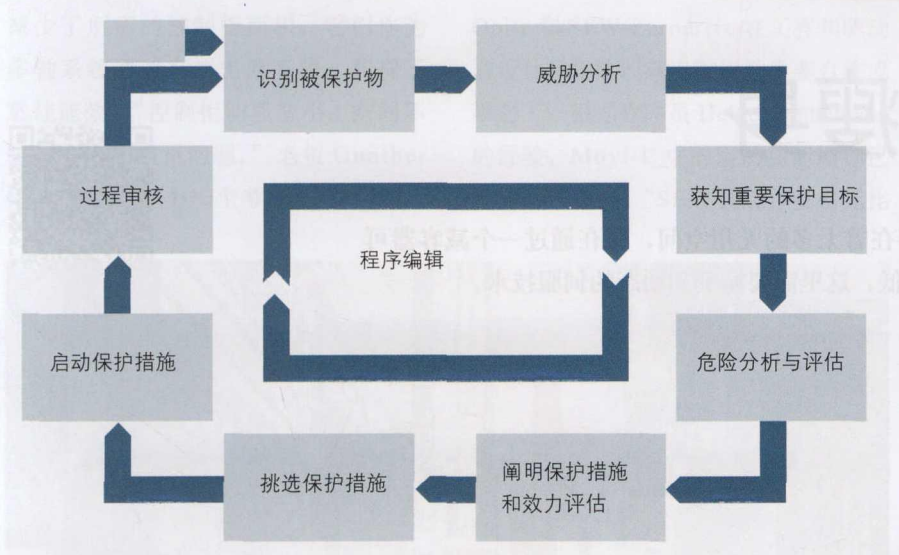


图 2 IT 安保程序模型

只能由从业者在特定情况下的外界支持下逐一完成。

相对应的技术和组织方面的保护措施制定和利用至关重要。在信息安全管理系统的基础上，后续的发展和维护是不可或缺的，这样可以维持或改善现有的保护等级。为了达到这个目的，所有参与设定和运行自动化解决方案的相关机构必须协同共进，这一点在国际标准 IEC62443 中做了阐明。

零部件生产商必须考虑到产品的安全性，其安全的组合运作必须被设备制造商所重视。操作者仅仅负责安全的操作流程。官方的安全程序与系统的操作相配合要试着关闭每个人入侵关口。对于入侵者来说，一个薄弱点就足够了。

重视功能性要求和程序

具备 IT 安全性能的产品和解决方

案的可利用性是一个安全设计的基础。在这方面，功能性和相应的程序极为重要：

●通过性能保护安全

在制定自动化解决方案的时候必须考虑到操作者的安全要求，为此就要进行自动化解决方案的威胁和危险分析。通过分析推导出对系统和投入使用零部件的要求。通过安全级别“SL”来选择安全性能，包括 1 级（误操作保护）到 4 级（强入侵保护）。国际标准 IEC62443 的第 3-3 和 4-2 部分阐明了各个性能和他们的协同作用，还包括了问题的辨别、利用控制、系统融合、信任度保护、数据流控制、监控和能源可利用性。

●以安全为质量

和性能同样重要的是对入侵者的抵抗力，其体现在运用时尽可能全面地避免薄弱点。这一点体现在 IEC62443 的

第 4-1 部分结合对安全的产品使用寿命的要求上，具体来说涉及到针对设备进行危险分析、安全实现和有针对性的安全测试。为了达到安全的产品使用寿命，必须设定相应的程序，人员必须经过培训。

IT 安全产品开发者的任务不止于提供给客户。因为产品不是 100% 完美的，产品开发者必须拥有一支产品安全事件责任团队，在发现薄弱点的时候制定解决方案并把信息传递给客户。关于系统融合方面在标准的第 2-4 部分给出了重要的质量参数。必须保证的是，解决方案要尽可能的不出现安全问题。除此之外，方案的提供者必须具备在制图、运用、文字和维护方面所需的安全知识和安全能力。因为安全措施只有在使用的时候才能体现出优点。建立防火墙要比没有好。总体来说当涉及到相应的受保护的规则时，它提供了一个很好的保护。

●安全使用

最后设备的操作者必须在操作流程和人员培训方面遵守安全规范。设备所能达到的保护等级不仅取决于设备本身的技术性能，也与长期的监管和维护有关。比如熟知设备的安装和性能其中包括一份网络计划和一份官方零部件的清单，还有对用户权力和登陆数据的电子密钥的监管。

一些“典型的”错误有不可撤消的额外连接或进入，不能更改的密码和已注销用户的识别码一直处于激活状态，每个错误都可能成为被侵入的薄弱点，而通过技术措施可以降低设备的可销售保护级别。

建立安全系统

为保障自动化解决方案防止被侵入需要获知所有参与者的系统操作。对于侵入者来说一个薄弱环节就足够可以引发巨大的危害。因此安全措施必须全面建立起来。为实现这一点 Phoenix Contact 的专家们可以提供咨询和支持。[MM]