



据联邦德国内务部称，现在每年通过对计算机物理系统的攻击就给德国带来 500 亿欧元的经济损失

工业 4.0

工业制造的安全战略

工业 4.0 的制造要求生产流程高效、连接很少和一个借助于全面的机器 - 对 - 机器 - 信息交换 (Machine-to-Machine-Kommunikation) 的前瞻性的机器设备的维护保养。为此，人们既需要一个稳固的安全战略，以消除如有害软件和工业间谍的威胁，又需要 IT- 服务商能够为此提供帮助。

文 | Thomas Schmidt

短短几十年来，电子行业和 IT 业在显著的改变着我们的日常工作，从而唤起了下一次工业革命：现在，通过 IT 大面积的进入制造业生产流程，发生了一个示范性的改变，这种改变召唤着如人们急切期待的工业 4.0 或第二个机器时代这样的概念。为了准确的回答生产的状况，迄今为止安装在生产的 IT 部件仍然受限于只能实现短的系统应答。也就是说：以前所建立起的机器与 IT 基

础设施之间的联系在时间上很受限制且不能直接对生产产生影响。

而今天，这些已经改观：单个的机器部件始终相互集成、产生测量值，并沿着整个生产链将其数据提供使用 - 而且这是超越地点限制的。而这便形成了一个办公和生产 -IT 的具有决定性意义的混合：客户订单委托系统实时的与机器进行数据交换、并操纵和控制着生产流程。

M2M- 数据交换的机遇与风险

今天，在短的机器生产状况应答方面，出现了各种不同的 IT 部件的高效连接，而这成了自动化生产制造的前提，并为工业带来巨大的发展潜力。这便实现了通过实时的机器对机器的信息交换 (Machine-to-Machine-Kommunikation) 对以往静态 - 线性生产流程进行持续的生产作业的控制。这便实现了在制造符合客户专门要求的个性化产品的生产流

程中所需的最大程度的灵活性。与此同时,也可实现在接下来的生产步骤中平衡加工作业的精准性,由此便减少了在加工过程中需剔除的不合格加工件的数量。除此之外,由于机器可行监控本身的磨损状况并能及时进行报告,这样最终避免了因需要维修保养机器的停机时间:这里的关键词是预测性机器维护。

但是,机遇如此大,那么也不能排除存在着风险。所有生产中的重要部件的持续联网,也加大了生产制造中不受欢迎的侵入的潜在风险。例如,美国国家安保局(US-amerikanischen Department of Security)的工业控制系统电子计算机控制紧急事件响应组(ICS-CERT)登记的工业控制系统的存在有侵入风险的部门在急剧增加。在此期间,已有850个部门在美国国家安保局(US-amerikanischen Department of Security)的

工业控制系统电子计算机控制紧急事件响应组(ICS-CERT)有登记附注。这850个部门中只有20%是2011年之前作的登记附注,剩下的80%的部门是在过去的4年中在美国国家安保局(US-amerikanischen Department of Security)的工业控制系统电子计算机控制紧急事件响应组(ICS-CERT)进行登记附注的- 仅在今年当年,就有85个部门在美国国家安保局(US-amerikanischen Department of Security)的工业控制系统电子计算机控制紧急事件响应组(ICS-CERT)有登记附注。德国工业也经受着类似强烈变化的威胁。据德国联邦信息技术安全局(BSI)称,10个最大的工业控制系统电子计算机控制(ICS)- 威胁中不再只是传统意义上的如通过互联网和局域网传染上有害软件病毒这样的IT- 安全防护- 风险。还有无数新的攻击

点,如必须注意连接互联网的控制部件或云计算- 部件的有损声誉的损害。据联邦德国内务部称,今天,每年通过对计算机物理系统的攻击所造成德国的经济损失就达500亿欧元,而官方未公布或未掌握的统计数字可能会更高。

中型企业成了主要攻击目标

人们会认为,这些数据不说自明。但是,在数字化时代,工业企业慢慢意识到,安全风险在不断加大,特别是中型企业更是这样。正是在工业4.0时代,中型企业成了主要攻击目标。因为,中型企业的人们常常是坐在工业产品的重要的界面前,其企业利润常常是7位数或是8位数的增长。但是,这些企业的安全水平如此之低,以至于一旦成了攻击者的目标,逃脱的机率甚微。

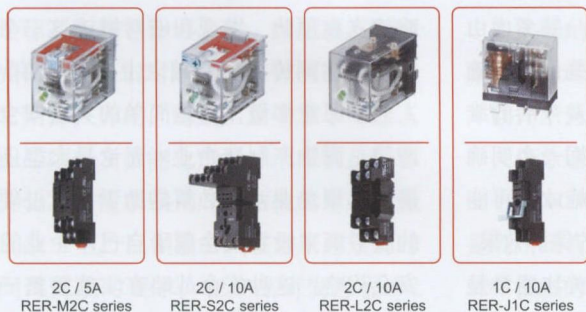
大型集团公司通常设自己的安全部

产品可靠 选型更简单!!

町洋国际通用标准继电器



- ▶ 体积小, 额定容量高。
- ▶ 提供带点动或旋转自锁按钮, 所有提供标准配置的动作指示窗。
- ▶ 结构合理, 用途广。
- ▶ 多种规格配有双向指示灯装置。
- ▶ 触点使用工业用银镍合金。



需要帮助?

请联系 DINKLE 或授权分销商或访问: www.dinkle.com
或 www.baidu.com 搜索 “DINKLE 授权分销商”

DINKLE 因联结而喜悦!!
Delight Through Connections

广告

门，这些安全部门给这些大型集团公司的中型供货商以支持。这当然是很糟糕的。原因是，长期以来，经济型企业是黑客喜欢攻击的目标。这样便形成了一个真实存在的影子经济。黑客由此便找到了攻击生产系统的弱点，并将其以六位数的价格卖出。在工业 4.0 时代，黑客有目标的攻击生产系统变得更加简单，目的是用他们找到的生产系统安全漏洞来敲诈这些生产企业，或是实施破坏，以损坏其竞争对手。这里有这样的生产系统遭受威胁情节脚本。如人们早些时候非自愿的唤醒了 Stuxnet 蠕虫，尽管这些原本完全是为其它环境所设计的，但是，Stuxnet 蠕虫一直在循环运行中存在并损害工业基础设施。无论是愿意还是出于不经意：如果一个系统被黑客黑过一次或是染上了病毒，这样，要重新清除生产 -IT 的病毒，会导致整个工厂不得不停产多日。严重的情况是，如果该集团公司由于连接生产、办公与 IT 从而形成了一个持续的病毒再传染，这样甚至会涉及到该企业集团设在世界各地的所有生产厂。有一点是清楚的：这就必须付出昂贵的代价。

必须将安全视为一个持续性的流程

出现损坏时企业必须进行的一次性投资，为了与一次性投资相比能够将花费减少很多倍。对此，如果众所周知该企业不相信自己能够挽回损失，那么就需为一个能够持续保护生产的稳定和全面的安全战略投资。没有专业过硬的咨询公司要实现能够持续保护生产的稳定和全面安全战略几乎是不可能的。原因是，在全面的数字化和工业生产情节联网的时代，安全不再是如同购买一个软件那么简单，这是一个持续性的流程。

如 Cancom Didas 公司这样的工业安全专家们会在从实际分析、准确的安全需求测试，再到安全措施的实施直至查验这样一个持续性的流程中陪伴着中型企业。在此，最重要的是首先要建立安全组织。接着要明确确定角色和责任，



所有生产中的重要部件的持续联网，也加大了生产制造中不受欢迎的侵入的潜在风险

因为在生产制造中，软件的高收益是一个新的很不寻常的事，而常常是，无论是 IT 部门还是生产部门均认为这不由他们负责。在这两个部门之间必须建立起一个功能性的界面。

第二步是，更加准确的识别现有的资产；也就是识别应该使用什么样的系统和相互之间如何进行信息交换？在此，重要的还有，要准确的判断它们的安全重要性：在整个增值链中，一个系统出现的安全故障应按怎么的标准进行判断？

由此便出现了一个关于安全的可能性方面的问题：企业内部的 IT- 基础设施提供怎样的手段、使用那些生产厂家的产品？采用了怎样的保护生产的相应软件？当然，在此还始终要一并考虑由此产生的费用问题，以及这些保护措施的实际作用和重要性如何以及今后的维护和保养由谁负责。只有根据一个明确的风险评估所制定产生的措施才有可能在节省成本的同时取得最佳的保护效果。

从技术方面看，人们的关注通常是在所有网络的逻辑或物理的分离方面：如同各部机器设备之间不需要联网那样，所有非强制性的必要的生产 - 和办公 -IT 的连接同样也应该分离。只允许通过可

控的安全机制进行信息交换。这样，当一部机器被侵蚀时，可阻止整个生产循环周期不会受到传染。

预防、发现和应对措施

然而，至今人们采取的预防措施还是不够的。应该如何识别可能发生的安全事故，这个问题不是不重要。原因是，因为从今天的观点来看，如果要在任何时候都能够 100% 防护冗余的联网的生产流程看来还不现实。谁要是被理解为是被证实的安全防护的最佳流程的话，那就必须要考虑到为了排除危害应如何及时的识别外来攻击和采取怎样的应对措施这些问题。一个可以信赖的安全战略建立在预防、发现和应对措施这三个方面均达到协调的基础之上的。所有，人们不愿意多做，而是简单的买进安全产品。而生产制造企业 - 无论是大型还是中小型企业 - 都必须借助于专业过硬的服务商来设置完全属于自己本企业的安全战略。这种安全战略在实施整整一年以后，企业的工业生产才能建立起一个基本的安全保护；从而最终建立起全新的角色和流程。而现在正是这场赛跑的发令枪打响之前的最后时刻。[MM]