[13] 刘群英，刘俊勇，刘起方 . 基于支路势能信息的电网脆弱性评估 [J]. 电力系统自动化，2008，32（10）：6-11.
Liu Qun-ying，Liu Jun-yong，Liu Qi-fang. Power Grid Vulnerability Assessment Based on Branch Potential Energy Information[J]. Automation of Electric Power System，2008，32（10）：6-11.
[14] David Watts. Security &vulnerability in electric power systems[C].NAPS 2003,35th North American Power Symposium, University of Missouri-Rolla in Rolla,Missouri，2003：559-566.
[15] 杨丹青，张学毅，邓杰，等 . 无人值班站电力调度电话实现方案的分析 [J]. 新型工业化，2015，5（9）：26-30.
YANG Dan-qing，ZHANG Xue-yi，DENG Jie. The Unattended Station Analysis of Electric Power Dispatching Telephone Implementation Scheme [J]. The Journal of New Industrialization，2015，5（9）：26-30.

实施工业物联网的 5 大挑战

物联网已经成为当世焦点及未来发展趋势，作为计算机和通信技术融合创新的产物，物联网及其“智能”设备不仅改变了人机交互方式，而且也让机器与机器之间的交互方式发生了变革。

我们看到物联网已经开始渗透到各个领域，其中普及速度最快和范围最广的垂直领域当属工业。事实上，能源、医疗、汽车和其他很多行业都在积极采纳工业物联网，诸如传感器、机器人、混合罐和胰岛素泵等设备越来越多地连接在一起。如 Tripwire 的安全研究和软件开发工程师 Lane Thames 的博客文章所述，物联网的这个子集也就是工业物联网未来有很大的发展空间。

泰晤士报认为“工业物联网将彻底改变未来，而不仅仅是工业系统，并且也会对许多相关人员造成巨大影响。如果我们能够实现工业物联网愿景的全部潜力，许多人将有机会通过无数的价值创造机会来改善他们的职业生涯和生活水平。”

泰晤士报继续指出工业物联网如何创建一些新的“智能”范例，如智能电网和智能医疗保健，以及具备自我意识的自动化机器驱动的新制造业生态系统的开发。

显然，工业互联网可以有一个光明的未来。但正如泰晤士报及时地警告说，“千里之堤溃于蚁穴”。 安全顾问 Larry Vandenaweele 观察到，连接到互联网和网络的设备可能威胁到我们的工业控制系统 (ICS)。这些系统对公用事业、能源和核能部门的运营至关重要。 更具体地说，随着业务需求的扩展，“智能”设备仅仅作为控制手段的界限将被打破寄云工业物联网，当工业物联网融入办公环境时，挑战与障碍也随之而来。

实施工业物联网时，行业将面临众多挑战。这里有五个特别突出：

主要挑战 1：解决设备功能

Belden Inc. 负责监督 ICS 研发和基础设施安全解决方案和产品的安全首席架构师 Jeffrey Caldwell 表示，今天工业物联网所面临的最根本挑战之一是制造者和过程控制操作员需要使用大量不同的设备和功能。

“工业领域已经有许多的机器对机器 (M2M) 互连和通信的解决方案，而且还有更多的方案产品不断的投入市场。”Caldwell 说，“因此在部署供邪物联网技术时，我们必须考虑几个问题。应该收集什么信息？信息应如何存储？如何最好地分析信息？应该根据分析做出什么决定？”

虽然对经济价值和投资回报率的分析可以帮助行业决定在哪些环节纳入工业物联网技术，但是解决能力的挑战一直延续到设备制造商。Joel Langill 是具有近 35 年工业自动化和控

（下转第 46 页）

[13]形形色色的核电站 [J]. 环境，2008，12：52-53.
All kinds of nuclear power plants[J].surroundings，2008，12：52-53.
[14] Yuri B.Shtessel. Enhanced Sliding Mode Control of the Space Nuclear Reactor System.Proceedings of the 34th Conference on Decision & Control,New Orleans，1995，12.
[15] Jose Alvarez-Ramirez，Hector Puebla，Gilberto Espinosa. A cascade control strategy for a space nuclear reactor system[J].Annals of Nuclear Energy，2001，28：93-112.

（上接第 38 页）

制开发经验的运营安全专业和工业控制系统网络安全顾问，以及信息共享网站 SCADAhacker.com 的创始人，他解释说，一些制造商仍在不断的解决工业物联网事物的复杂需求。

“我所谓的‘制造完整性’的真正风险是，当可能非常适合典型办公环境的产品和服务，被拿来在制造环境中解决相同的问题，而没有全面考虑工业环境相关要求（环境、危险区域、可靠性和服务可用性等）”Langill 解释说，“最后，工厂环境的控制组件（控制器、传感器、执行器等）在物理空间层面的连接仍然基于传统 IT 架构，这些架构在工业网络中并不常见。虽然以太网（注意我没有说 TCP 或 UDP）与几十年前相比，应用已经非常普遍，但它与 Windows 平台在工业环境中几乎没有多少应用，因为它们不能满足最基本的工业运营要求。

对工业物联网的落地规划，不仅个别工业企业必须认真考虑到要实施工业物联网的地方，制造商也要明确定义运营要求，了解他们希望得到的技术和能力。这需要深刻理解最终需要应用工业物联网技术的实时生产设备。

关键挑战 2：供应链关系

功能不是制造商在未来几年需要解决的唯一焦点。成本和工业可靠性也将作为早期采用者争取向工业物联网过渡时需要考虑的一部分。随着嵌入式系统越来越多地进入企业，制造商有责任保持他们供应链的完整性。

Patrick Miller 致力于全球关键基础设施的保护和防御，对工业物联网供应链的完整性保持有自己的看法。Miller预测，“特别是在关键基础设施中使用工业物联网元素时，我预计政治、舆论和其他方面开始关注供应链的完整性。为了摆脱这种潜在的阻力来源，组织必须考虑如何最大程度地最大化制造过程中的透明度和标准化。他们将需要根据商定的开放标准来构建设备，该标准可以独立评估，以确保仅包含预期的硬件，软件或固件。”

关键挑战 3：安全

与工业物联网设备的组件完全相关的是研究人员为确保它们而采取的措施。 Access Control Technologies LLC(ACT) 总裁兼管理成员以及 Tripwire 业务开发合作伙伴 Ron Carr，有超过 40 年管道 SCADA 通信的管理经验，他认为安全问题不仅影响制造商和过程控制运营商，还有管道控制操作员。

他表示：“网络通信所控制的任何设备和系统在面临互联网的时候，都处在遭到黑客入侵的威胁中。”工业物联网设备也绝对不会被免除这种威胁。例如，根据 Carr 的说法，“为了下载软件升级，将流量计算机接入笔记本电脑（有互联网连接），在这短暂的时间内就有可能被上传恶意软件，如 BlackEnergy 或 Stuxnet 就属于这种类型。

为了防范这些和其他威胁，工业企业应考虑如何将高级网络威胁防护解决方案整合到其网络中。

关键挑战 4：弥合我们的优势

（下转第 63 页）

Maintenance，2002，12：39-41.
[5] 彭欢 . 基于 V5 Automation 的 CATIA 二次开发技术研究 [J]. 电子机械工程 ,2012,(02):61-64.
Peng Huan. Research on CATIA Secondary Development Technology Based on V5 Automation [J]. Electronic mechanical engineering，2012，（02）：61-64.
[6] 牛文兴 . 三维零件库的设计与实现 [D]. 天津 : 天津大学，2003.
NiuWen-xing. Design and Implementation of 3d Spare Parts Library [D]. Tianjin: tianjin university，2003.
[7] HaoZouling，Guo Dong-ming，Gao Hang，et al.A Method to Analyze the Difference of 3-D CAD Model Files Basedon Feature Extraction[J]. Journal of Mechanical Science andTechnology，2011，25（4）：971-976.
[8] 李琼 . 面向制造特征的加工方法研究 [J]. 新型工业化，2016，6（11）：75-80.
LI Qiong. Study on the Processing Methods Oriented to ManufacturingFeatures[J]. The Journal of New Industrialization，2016，6（11）：75-80.
[9] 叶恺 .Access2010 数据库案例教程 [M]. 北京：化学工业出版社，2012.
Ye Kai .A Case Study of the Database in Access2010 [M]. Beijing: Chemical Industry Press，2012.
[10] 陈宏钧 . 简明机械加工工艺手册 [M]. 北京：机械工业出版社，2008.
CHEN Hong-jun. Concise Machining Process Manual[M]. Beijing：China Machine Press，2008.

（上接第 46 页）

在实施工业物联网时，安全性是一个非常重要的问题。然而，与任何新技术一样，技术问题仍然无法解决人员分裂等问题，并阻碍了人们更好的协同工作。

“也许克服的最大挑战是破除不同学科和部门之间的障碍。”业界领先的自动化、控制、软件、制造、市场营销和领导力作家 Gary Mintchell 说，“多年来一直在讨论的著名的‘IT/OT 融合’必须实现。控制工程师必须升级他们的技能，使他们知道网络和安全至关重要。IT 工程师和架构师必须了解业务流程与制造流程之间的区别。”

要实现这一点并不容易，然而，建立新的协作机制将使整个企业在生产力、盈利能力、客户服务和可持续性方面受益。正如明茨尔正确地指出的那样，“领导者必须加强他们的能力以引领整个行业的发展”。

关键挑战 5：安全

实施工业物联网时企业面临的第五个也是最终的关键挑战是安全。这种担忧源自于互相连接的设备以及物理控制的深度整合引入了新的攻击方式。

Tripwire 负责解决方案和战略的安全和信息技术风险策略主管 Tim Erlin 阐述：“当然，工业领域的安全规定有着悠久的历史，但它们很少考虑到逻辑攻击会带来哪些物理的影响。我们已经看到了 Stuxnet 和德国钢铁厂的这些“动态网络攻击”的开始，令人担忧的是工业物联网的快速增长让越来越多的工业场景暴露在网络安全威胁之下。工业网络安全与 IT 安全性不一样，我们需要新的方式来应对这种新的挑战。”

幸运的是，工业企业可以通过 IT 与 OT 之间的融合与平衡，来应对这一安全障碍。“我们必须追溯 OT 领域的历史以及相关运营者的经验，”Erlin 建议。“IT 安全小组应该开始将工业安全纳入其威胁建模，并开始与 OT 安全小组就如何做到这一点进行磋商。这不是 IT 或者 OT 小组能够单独解决的，而是需要二者的共同努力以实现双方完美融合。

结论

实施工业物联网的关键挑战似乎都是艰巨的。然而，与设备能力、供应链关注、安全性、人与人之间的分离以及安全相关的问题，所有这些最终都将显示出部门、整个企业和制造商必须共同努力，才能在技术不断发展的情况下时刻把握住正确的方向。以上我们提到的 5 个方面，都有相应的适合某个行业可用的方案，但采取哪种方案取决于每个行业组织的选择。