

数据传输

安全可靠的数据传输非常重要

对于工业 4.0 而言，数据能够安全可靠地传输非常重要。在此，数据必须能够防护外来的攻击（防护）。迄今为止，人们更多的时候只是重视工作安全的可靠性（安全）。为此，机械设备制造厂商和专业 IT 人员必须共同合作，以确保数据能够安全可靠地传输（图 1）。

文 | BARBARA STUMPP

近年来，几乎所有行业的生产都处于订单产品数量下降但产品多样性上升的状态。而现在工业 4.0 帮助此类生产更具经济效益，即新兴的生产项目在经济上也能有所收益。IT-Bitkom 协会的一项研究表明，实行工业 4.0 后，到 2025 年，仅机械和设备制造业、电子工业、汽车制造业、化学工业、农业及信息和通信技术行业将增加的所创造价值潜力拟可达 780 亿欧元。

实行工业 4.0 理念，即企业需要改变原有生产结构，以网络物理系统（CPS）

为基础，打破生产地点的限制，自行进行生产和物流运输，而相应的必须能够从控制制造方面进行信息交换和编程。在此，CPS 必须具备“安全”及“防护”功能。

没有设置主密码

Fanuc 德国公司的技术负责人 Mathias Fritz 先生表示：“对于控制而言，重要的是要将信息的安全性和功能性与企业安全相结合（图 2）。与安全关系重大的观点是，通过一个机密的密码保护

和一个验证号测试阻挡来自外部的操作，正如 PMC（可编程控制器）程序通过单独设置的密码来加以保护。在此不存在控制生产厂商设置主密码。这样企业的安全技术就可以阻挡对外来的控制。”

必要的灵活性要求具备绝对联网；病毒对软件，对 Stuxnet 的攻击在这里找到了突破口。为此，企业开始设置相应的程序。在此，Bosch Rexroth 公司、B&R 公司、Fanuc 公司和 Mitsubishi 公司已经拥有具备完整功能性的安全可靠措施。控制装置需具备在工业 4.0 前提

图 1 实现工业 4.0 的前提是，机械设备的具体部件之间的信息交换不仅是安全，还必须做到防护



下，在复杂的情况中加工处理大量数据的能力，并需要很多公共界面，目的是为了和 Ehternet、Profibus 及 CC Link 等标准交换信息，并使传感器层面的界面和图像系统的界面相互交换信息。集成化的数据库功能必须与对一个主服务器的数据自动化回复或是对一个包括与互联网和云计算联接的数据库数据自动回复。这包括了通过 PC 进行数据存取或移动信息交换装置在 SPS 上通过企业系统进行数据存取。

IT 部门需要作出调整

在一家公司建立了 IT 安全方法，原则上必须要传达给 IT 部门。具体表现在 IT 部门需要作出的调整。如这在工业基础设施中会呈现出另外一种情况，必须与在企业 IT 中实时发生的情况有所区别。



图 2 Fanuc 德国公司的 Mathias Fritz 先生表示：“对于控制而言，重要的是要将信息的安全性和功能性与企业安全相结合。”

Bosch Rexroth 公司产品销售管理部门负责人 Norbert Sasse 先生解释到：“在



图 3 Bosch Rexroth 公司的 Norbert Sasse 先生表示：“在这里，首次建立了 IEC 62443 标准（IT 安全的工控网络与系统信息安全标准）的工业安全防护评估标准框架。”

这里，首次建立了 IEC 62443 标准（IT 安全的工控网络与系统信息安全标准）的工

慧于心、简于行 — 魏德米勒 u-remote



Weidmüller

魏德米勒 u-remote 通过现场总线及工业以太网，将现场的安全装置和核心安全控制器联接起来，构建成一个完整的安全系统。安全型输入和输出模块可以完美的应用于离散式架构中，实现安全可靠地设备关断。

- 紧凑的设计，高密度的联接
- 4DI-4DO 安全模块结合各种安全功能仅 11.5mm 宽
- 多功能的安全模块使安全系统规划更简单

浏览 www.weidmueller.com.cn/u-remote 了解更多关于魏德米勒 u-remote 信息

魏德米勒电联接(上海)有限公司

电话: 86 21-22195008 网址: www.weidmueller.com.cn/u-remote

扫一扫，关注魏德米勒官方微信



Let's connect.

业安全防护评估标准框架（图3）。在此重要的是，起着关键性作用的是要建立工业部门数据安全防护意识的措施。”

尽管企业的专业人员已经达成共识，也就是数据安全防护仍然是一大问题。“从工业4.0角度出发，为了防范外在危险，保证数据的传输安全，未来不再有独立界面和封闭数据模式（图4）。”B&R公司市场经理Stefan Schönegger先生表示，“这里特别涉及到一个开放的Ethernet数据交换与基于实时的机械设备控制与非实时应用的连接，如基于Web的应用或云计算服务。”为此，Bosch Rexroth公司为其用户提供了工业安全防护指南。”

设计安全防护非常重要

重要的是，建立集成式用户友好型安全防护技术方案、结构和标准，在整个生产流程中允许准确且可靠的一致性证明产品、生产流程和机械设备与可靠的信息交换。在各种情况下，设计安全防护都非常重要。也就是在规划和拟定设计阶段就要考虑到IT的安全性。

在Mitsubishi公司和Fanuc公司，考虑到了Windows的病毒和类似易得的病毒并实行一个极端的分离。Mitsubishi Electric Europe公司高级业务发展经理Thomas Lantermann先生说：“我们为用户提供一个系统，用户可以选择是否使用云计算支持，而直接与其MES/ERP交换数据（图5）。”

为此Mitsubishi公司研发了自己的快速网络，目前还有很多用户对云计算不甚了解。Mitsubishi公司的Lantermann先生表示：“我们的云计算服务器和SPS提供的是，与互联网、云计算再加上互联网信息传输协议和安全保护，是这样基于一个安全可靠的实时操作控制系统，而非基于Windows系统。这样我们的用户便按照他们的意愿使用互联网。”Mitsubishi公司称此项解决方案为开放式防护。

Bosch Rexroth公司的开放式酷睿技



图4 B&R公司的Stefan Schönegger先生说：“从工业4.0角度出发，为了防范外在危险，保证数据的传输安全，未来不再有独立界面和封闭数据模式”

术能够全面覆盖使用相应的软件工具的基于SPS的技术范围。开放式酷睿交互界面架设了由SPS通往IT的自动化桥梁。

实时地进行数据交换

Matthias Fritz先生说，在Fanuc德国公司，人们将实时数据交换称作无缝链接概念（Seamless Concept）。“完全相同，工业4.0以怎样的表现形式进入生产车间，我们必须既要建立一个控制层面的标准化平台，又要实现用户的个性化匹配。Fanuc德国公司使用Seamless Concept扩展到可以用于所有的标准化CNC。该实时数据交换方案的一个部分是，创造条件使信息交换程序和生产制造流程中的数据交换要尽可能的实时进行，为此程序处理器/CPU要分开使用。”

对此，B&R公司的Stefan Schönegger先生表示：“我们致力于开放式解决方案和Powerlink。Powerlink能够可靠且不受外部影响地严格按照时间要求来传输实时数据。对时间要求并不严格的数据如组态数据或网页服务数据可集中由分开的信道进行传输。这同样也处于通过开放式防护数据交换状况。”

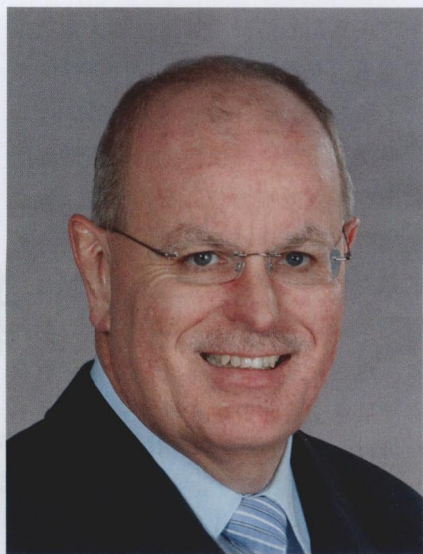


图5 Mitsubishi Electric Europe公司高级业务发展经理Thomas Lantermann先生说：“我们为用户提供一个系统，用户可以选择是否使用云计算支持，而直接与其MES/ERP直接交换数据。”

工业的Ethernet协议

在寻求标准方面，许多公司使用OPC UA或像Bosch Rexroth公司和B&R公司这般工作。OPC UA（OPC统一构架）是一个关于机械设备间进行信息交换的协议，从当前版本的OPC UA看来，该协议不仅可以传输机械设备的（流程值、测量值和参数），且机械设备还能将语义表述出来。

OPC UA基于一个面向服务的体系结构。OPC UA的一个新特点是具有冗余性。在此，有一个两个方向的连接监控，这样服务器如用户能够发现连接中断。首先是在连接中断时不会丢失数据。OPC UA的应用证明了网络防护方案有效，且能够保护网络，使得未经许可不能进行网络的信息存取处，并能够保护网络不受破坏和随意操作。

在工业4.0能够发挥功能之前，人们还需要完成大量的研发工作。如何接近理想状况，技术可行性的占比较小，更多的取决于参与工业4.0研发的企业在这方面的投入所获得的性价比如何，并取决于参与到工业4.0研发的企业对所参与的研究投入。MM