Rockwell Automation

为第四次工业革命保驾护航

零信任策略确保 OT 领域数字化转型安全无虞

引言

数字化转型是推动技术进步与效率提升的关键因素，同时也带来了经济层面的颠覆，深刻影响着组织的创新和发展节奏。

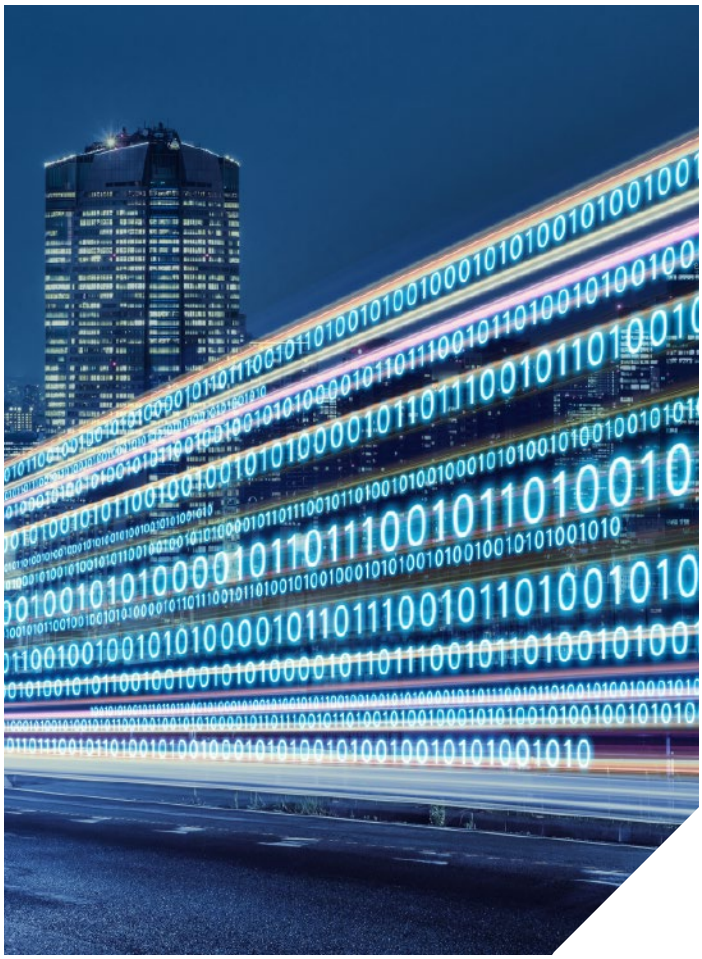
想要应用数字技术革新产品、服务和业务，就得获得更深入的洞察力和控制力来提升效率，而这往往需要利用新的数据流。实施上述工作会带来全新的体验（如客户体验），同时改变原有运营模式，对数字资产安全性产生积极影响。

在运营技术 (OT) 领域，数字化转型正在推动两大变革：

- OT 系统正在接入以往从未涉足的网络，以便提取运营方面的新数据。根据定义，这些系统处于基础设施的“边缘”位置，因此必须作为端点进行部署、保护和管理。
- OT 生产环境中也在部署富数据软件应用程序，确保新数据得到充分利用。由于数据量太大和带宽问题，可能会导致数据处理速度延迟。为了解决此问题，还会将应用程序部署在端点处，并进行保护和管理。

此外，OT 组织还面临其他足以影响安全性、必须在现代化升级道路上加以解决的常见挑战。

1. 即使是较新型号的过程传感器，也没有自带安全功能和设置密码。在最近发生的一个案例中，一家领先供应商刚刚向阿联酋出货了 3,000 个未加密的新传感器。
2. IT 网络安全供应商通常解决第 2 至 7 层的安全问题。这适用于大多数 IT 网络。但 OT 威胁往往通过第 0 至 1 层传播，在这些层级无法进行遥测监控，因此检测不出威胁。
3. OT 安全最终由谁负责仍不明确。理论上讲，OT 安全应由首席信息安全官 (CISO) 负责，而且有许多行业组织正在将这一职责分配给 CISO。然而，鉴于 CISO 对车间运营的了解通常很有限，而车间主任作为车间管理者，一般不会轻易放权给 CISO。
4. 美国运输安全管理局 (TSA) 的管道网络安全指南不涉及控制系统，包括传感器。但在网络安全和基础设施安全局 (CISA) 看来，TSA 应负责管控整个能源网络。
5. 美国石油协会标准 1164《管道控制系统网络安全》（2021 年 8 月）将过程传感器排除在外（第 6.6.5.4 (b) 条），规定“未联网仪表不包含在资产盘点范围内”。



尽管 MITRE ATT&CK 工具、CVE 方法等效果显著，但我们还需要做更多工作。例如，MITRE ATT&CK 工具根本无法处理过程传感器和其他控制系统现场设备的问题，而针对软件漏洞的 CVE 方法也无法处理控制系统硬件的问题。

解读当今标准，消除标准中落后于 OT 威胁发展速度的防范缺口 —— 这项工作需要十足的耐心。

此外，为了保障安全数字化转型取得成功，IT 和 OT 部门必须在策略部署、安全以及过程变更管理方面通力协作。这确保最终可以安全、可靠、合规实现预期的生产力提升目标。

常见的数字化转型障碍

公司无法达成数字化转型目标有很多普遍的原因。在进行 OT 变革时，这些问题会被放大。

必须将互为孤岛的传统 OT 系统练成一片大陆。

传统 OT 基础设施中的“自动化孤岛”缺乏实现数据访问所需的基础。此外，针对工业环境的资产盘点不够到位，这会导致企业不清楚自己有哪些联网资产。

作为影响控制和安全系统以及操作员决策的因素，过程传感器无处不在，但不符合本质安全要求。由此会造成灾难性故障。这通常表示工程部门对原本就熟悉的安全问题的关注度要超过安防问题，因为工程部门认为解决安防问题是 IT 部门的职责。

反过来，IT 部门也倾向于忽视过程传感器安全性，将其视为工程部门的独有职责，不属于自己的职责范围。

但是，在过程传感器层面，安全和安防确实是同一个问题。

战略不一致或不明确。

数字化转型战略中必须包含协同工作这一项，为关键业务目标设定明确、可衡量的结果，同时维护所用关键数字资产的安全性，并确保符合行业标准。

路线图创造不出早期价值。

以业务成果（而不仅仅是技术）为导向，制定一个旨在实现数字化转型价值的短期和长期路线图是项目取得成功的重要基础。

主要利益相关方各自为政。

数字化转型需要进行组织文化变革。IT 和 OT 部门主管的思维模式必须保持一致，使两个利益相关群体共同成功推动项目的业务目标。

第一步是确定企业中需要保护的对象（数据、资产、应用程序和服务 (DAAS)），并设置优先次序。

深入了解过程传感器

服役时间已超过 20 年的传统系统通常无法在配备数千个过程传感器的物联网环境中运行，这本身就是安全漏洞。如果没有适当的规划和管控，实施现代化升级就会使网络安全风险成倍增长。

为什么保护过程传感器如此重要？

根据最近的一项报告：“网络安全威胁不断增加，导致传感器数据传输可能受到黑客攻击。必须了解被黑客入侵的传感器数据会如何影响设定控制性能。典型的情况可能包括传感器数据被黑客篡改并发送到控制回路，从而导致极端的控制行为。”

一些涉及过程传感器的网络相关事件包括：

- 错误的低水位数据导致水坝运转失常，最终崩溃
- 传感器导致 1,000 万加仑未经处理的废水被排放
- 核电站中的安全泄压阀因压力传感器从未达到设定值而不升起
- 佛罗里达州一家联合循环发电厂的一个电压传感器发生故障，导致该发电厂发生 200 MW 负荷波动，进而造成新英格兰发生 50 MW 负荷波动
- 液位传感器读数错误导致储油罐爆炸
- 传感器读数错误导致飞机坠毁
- 传感器读数错误导致炼油厂爆炸

缺乏网络安全、身份验证或网络日志功能的过程传感器使我们无法辨别此类事件是否存在恶意行为，因为它们看起来都是偶然发生的。

为便于了解过程传感器固有的漏洞，需要提出以下三个重要的安全问题：

1. 必须到现场才能破坏传感器吗？
   不，破坏行为可以远程完成。
2. 与网络相关的传感器影响会造成多大危害？
   现场校准仪一次只能校准一个传感器，但无法安全地连接互联网。资产管理系统 (AMS) 可以访问数千个传感器。与此同时，AMS 直接连接互联网也不太安全，而通常会连接到企业资源规划 (ERP) 系统。传感器问题导致灾难性故障的一个真实案例：Colonial Pipeline。
3. 当受损的传感器数据被发送到云端用于大数据分析、物联网或工业 4.0 应用程序时会发生什么情况？
   假设传感器数据没有受损。

由于肩负着实施安全数字化转型计划的重任，OT 部门需要解决过程传感器存在的缺陷，即了解威胁主体如何中断、降级或损坏和破坏基础设施；存在哪些风险和代价；以及可以采取哪些步骤来弥合漏洞。

零信任策略可消除围绕过程传感器的过度信任问题和风险。零信任策略的起始信任级别为零，通过该策略，可以完全了解企业中每个“实体”（无论是数据、应用程序、服务还是包括过程传感器在内的设备）的可信度并进行持续验证。

制定安全数字化转型规划

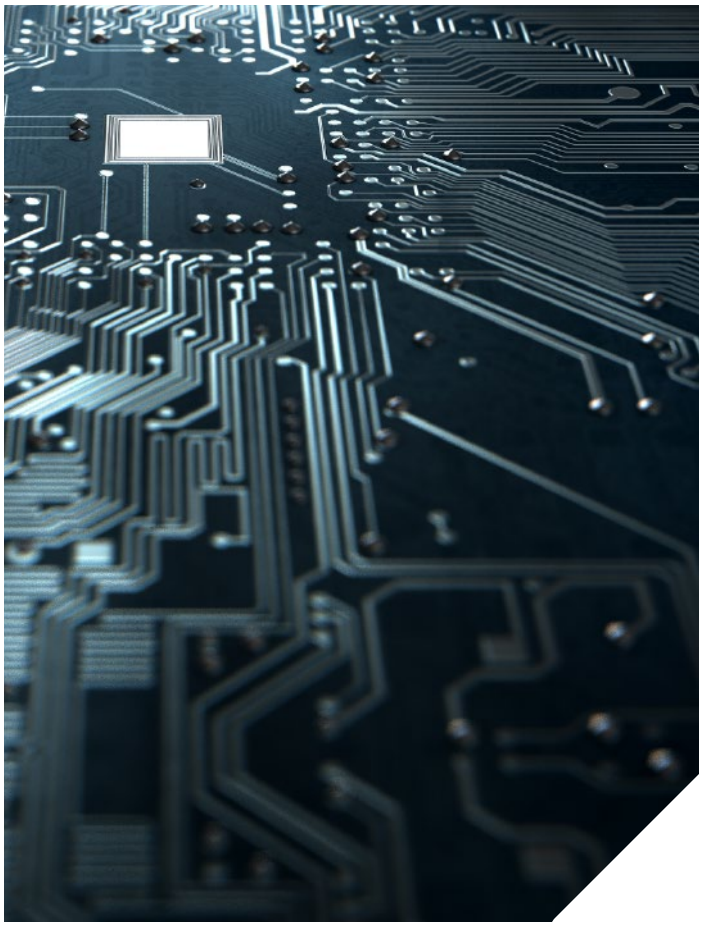
所有安全数字化转型难题在 OT 环境中都会被放大，这也就难怪工业组织在现代化方面落后于更加以 IT 为中心的行业了。

幸运的是，我们仍有行之有效的成功路线。

实现 OT 领域的安全数字化转型涉及以下几项关键策略：

- 零信任方法
- 合适的现代数字解决方案
- 改变组织内部的所有权责任制
- 改进常见和易受攻击资产（如过程传感器）的合规标准。
  替代方案是直接解决防范缺口。

虽然上述每一点都很重要，但零信任方法是本次讨论的重点。



零信任方法

零信任是在工业环境中部署安全数字化转型技术的绝佳策略。随着数字化转型趋向成熟，该策略支持新的用户群体、客户参与模式、快速应用以及新的 IoT 和 OT 设备与传感器——所有这些都采取了网络安全保护。

零信任基于五大设计原则，结合以下五个基本步骤能够有效推动整个企业的安全数字化转型：

1. 明确资产和保护面
2. 映射事务流
3. 设计架构
4. 实施策略
5. 执行持续监控与维护

明确资产和保护面。如零信任策略创始人 John Kindervag 所言："零信任是一种将业务战略与网络安全实践相结合的战略。" 通过关注业务成果，可将安全性视为促进因素，而不是阻碍因素。

第一步是确定企业中需要保护的对象（数据、资产、应用程序和服务 (DAAS) 元素），并设置优先次序。DAAS 元素对业务至关重要，每一个都应被优先对待。这些元素也被视为保护面，如 ICS 控制、IT 网络、客户信息数据库、知识产权 (IP) 数据等。

- 数据：基于数据对贵组织的重要性、对黑客的价值以及是否符合法规要求，对数据进行分类。将数据治理计划（全部，尤其是保护面内的）文档化意味着企业可以在有效的安全控制措施到位时识别、分类、传输、保留和处置数据。
- 应用程序：了解哪些应用程序使用了可能对威胁主体有价值的敏感数据或专有代码。设计必须由内而外完成。映射系统工作方式以及 DAAS 元素各组件与网络上其他资源之间的交互方式。了解通信流量在网络中的流动方向，特别是保护面中的数据，将有助于应用程序内和应用程序间数据保护策略的制定。
- 资产：创建详细的设备清单，包括笔记本电脑、手机、制造设备、PLC、IoT 设备（如过程传感器）以及其他联网资产，以便您知道保护面中要包含的对象。
- 服务：确定所有需要保护的关键业务网络服务，如活动目录、DHCP 和电子邮件。通常情况下，服务帐户应执行已知行为，并具备有限的连接权限。它们不应直接尝试访问域控制器或身份验证系统，并且任何异常行为在发生时都应被迅速识别并上报。

通过将网络安全防御集中在每一个保护面上，并根据其对企业的重要性进行优先级排序，可以创建比寻常的企业攻击面（可能被视为整个互联网）更小、更易于管理的防御边界。

每个组织都会经历多个数字化转型项目及相应的保护面。最初的转型计划规模小，但具有战略意义、影响力和可衡量性，可为企业提供零信任网络安全的实施经验，并为后续项目的成功提供框架。

映射事务流。工业环境的网络资产盘点通常不到位，导致企业不清楚工业环境中哪些对象应该联网以及实际又有哪些联网对象，从而产生漏洞。这些系统通常是自然发展的，在设计知识方面经常出现空白；或者假定的安全设备可能给网络带来未经保护的互联网入口。

要正确设计网络，必须由内而外进行。了解系统应采取的工作方式以及各个 DAAS 组件与网络上其他资源之间的交互方式至关重要。通过映射通信流量和相互依赖关系、将特定资源之间的交互方式文档化，以及将这些相互依赖关系应用到安全策略和控制中，您就能确定所需的保护类型和级别。

映射事务流和 DAAS 相互依赖关系，特别是与保护面相交的任何对象，可以实现更好的保护，而不会意外中断任何相关应用程序、服务或工作流。该步骤还为下一步做出更明智的决策提供了深入了解和必要信息。

设计架构。明确保护面并映射事务流之后，必要的零信任架构一般就会自我呈现出来。

零信任最佳实践要求安全控制措施尽可能靠近受保护的 DAAS 元素。否则，零信任架构就不会以某个通用模板为基础了。相反，它会利用多种网络安全工具和策略（取决于每个保护面）实现其目标。各企业必须在每个保护面部署和集成一系列功能，包括增强身份和访问管理、访问控制、网络分段、微边界以及 DAAS 元素要求的其他功能。

因此，零信任网络设计应基于网络中的事务流方式和往来于保护面的 DAAS 元素，并考虑用户和应用程序访问保护面数据的方式。可以根据优化后的通信流决定应使用物理和/或虚拟设备将分段和微边界部署在何处。

实施策略。在第四步中，将根据数据的预期行为以及与该数据交互的用户或应用程序为分段网关编写策略规则。

一旦设计团队确定了最优通信流，下一步就是确定如何在分段网关处实施访问控制和检查策略。数字化转型已经日渐成熟，企业洞察力不断发展，策略应该从粗粒度方法开始，随着对用户需求和业务需求了解的增进，策略也越来越细化。

零信任的一个关键原则是将访问限制到“须知”层面（即最低权限原则），并严格实施这种访问控制方式。为了定义这些规则，设计团队必须详细了解哪些用户可以访问哪些数据以及情境信息。

仅仅知道源地址、目标地址、端口和协议是不够的。安全团队需要了解已确认的用户身份以及应用程序——通常充当现代分段网关中数据类型的代理。

为了让资源之间进行交互，必须有专门的规则允许通信行为。制定该规则必须回答以下问题：

- 哪些人可以具备访问权限？该问题用于定义“已确认的用户身份”。
- 什么应用程序访问什么资源？已确认的用户身份使用什么应用程序访问保护面内的资源？
- 用户何时具备访问权限？何时尝试访问资源？
- 他们可以从哪里发起访问？数据包目的地是哪里？
- 我们为什么这么做？该数据包为什么试图访问保护面内的此资源？这关系到数据分类：从数据分类工具自动获取的元数据有助于使策略更精细。
- 我们该如何保护它？为了保护它，您必须要了解访问数据包的已确认用户身份是如何通过特定应用程序访问保护面的。

持续监控与维护。这是实施零信任方法的第五步。

此迭代过程意味着持续查看通过第 7 层的所有内部和外部日志，重点放在零信任的操作方面。通过发送尽可能多的环境相关遥测信息，获得关于如何逐步提高安全性和效率的新见解，以及如何为变革新领域制定有帮助的见解。

技术环境正面临无数威胁。企业必须保持持续监控能力，以确保他们能够实时了解环境中发生的情况。然后，网络受到的攻击越多，它就会变得越强大，因为该过程使策略更加安全，并且使迭代设计更适应为增强安全性所做的架构调整。

工业安全标准

OT 行业遵循四个主要安全标准。

- IEC 62443 工业自动化和控制系统 (IAC) 安全
- 国土安全部/工业控制系统网络应急响应小组 (ICS-CERT)
- NIST 800-82 工业行业 —— 国家标准与技术研究所
- 国土安全部/爱达荷国家实验室

每一个标准都是基于纵深防御安全架构，其本身就存在漏洞。此外，这些标准实际上并不是策略，而是一种战术部署，即通过一种基于工业非军事隔离区概念 (IDMZ) 的控制措施或产品解决方案来解决特定点的漏洞，而 IDMZ 就是制造或过程设备中的边界、缓冲区或“隔离区”，位于组织业务系统与工业控制系统之间，具有不同的安全要求，相互之间不存在固有的信任。

数字化转型改变了这两个系统的信任因素。如今，如果想要通过数字化转型开发的新商业模式互动获得成功并实现预期的积极成果，信任必须满足敏锐性、情境化和适应性要求。

罗克韦尔自动化遵循 IEC 62443 工业自动化和控制系统 (IACS) 安全标准以及零信任方法。零信任的设计原则完全符合 IEC 62443 要求，简化了合规流程，同时加强了对不断演变的威胁环境的防御。

总结

OT 行业的安全数字化转型可以利用零信任作为关键框架，确保转型项目在合适的网络安全保护下启动。

零信任和安全数字化转型之旅都应循序渐进地开展。数字化转型改变了工业控制系统和业务系统之间的信任因素，因此需要使用互补策略执行安全数字化转型规划，以提高效率和生产力，并在网络的每个连接点处实现全面的网络安全可见性，同时确保相关措施落实到位。

规划初始安全数字化转型项目，以及对项目中每个保护面内的 DAAS 元素进行识别、优先级排序和保护，都将帮助企业实现其早期价值，并建立网络安全保障模式以在转型期间保护组织。

全面保护

罗克韦尔自动化在复杂 OT 环境中的安全数字化转型方面拥有丰富经验。利用我们的专业资源可以帮助您设计、实施和监控您的项目，以实现更大的运营回报，确保从规划到生产全程采取合适的网络安全保护。

采取行动

深入了解安全数字化转型。

深入了解 OT 网络安全中的零信任策略。

与专家探讨如何开始这一征程。

关注我们。

rockwellautomation.com expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Allen-Bradley 和 expanding human possibility 是罗克韦尔自动化有限公司的商标。
不属于罗克韦尔自动化的商标是其各自所属公司的财产。

出版物 GMSN-WP003A-ZH-P – 2022 年 5 月

© 2022 罗克韦尔自动化有限公司版权所有。保留所有权利。美国印刷。