Siemens Digital Industries Software

数字线程中的数据保护

西门子与 Identify3D 联袂打造

高层摘要

Siemens-Identify3D 技术套件可以保护数字制造线程中数据的机密性和完整性，提供知识产权保护，实现可重复性和可追溯性，从而抵御不断演变的网络安全威胁。

简介

随着数字化制造在工业 4.0 和物联网 (IoT) 等计划中的兴起，用于设计、工程、生产和流程控制的各类工具现在都以数字方式关联到了一起。数字线程中的信息共享促进了整个产品生命周期内的协同，不仅提升了效率，而且削减了成本。然而，数字线程中的各种系统与软件之间需要通过数字连接，这就导致数字化制造生态系统面临着大量的网络安全威胁。

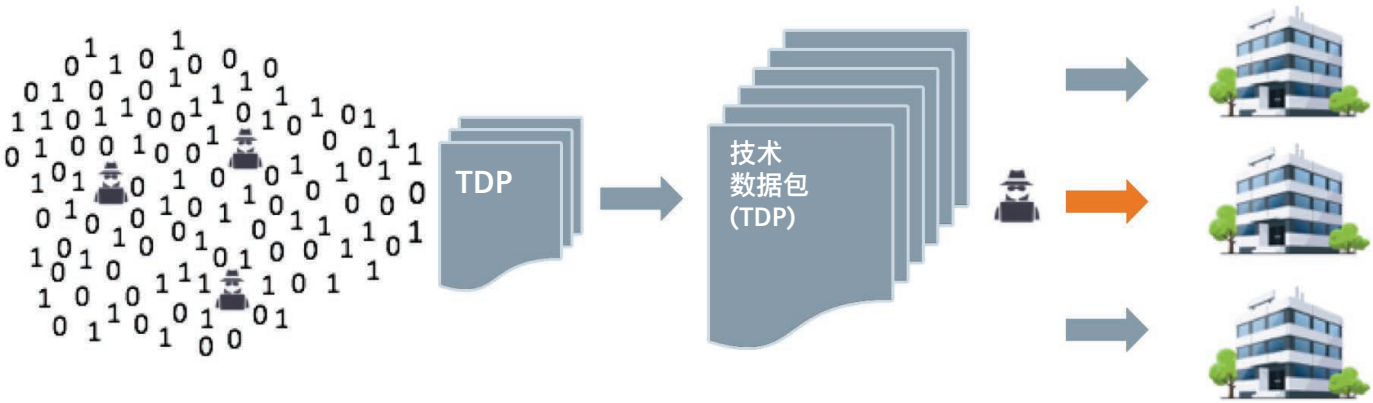
在设计和工程端，Siemens Digital Industries Software 提供诸如 NX ™ 软件等计算机辅助设计工具，可以对单个零件、整体装配乃至整个制造流程进行设计、仿真和可视化。通常，设计流程中利用的工具多种多样，而每一款都需要与流程中涉及的其他工具实现互操作性，才能尽可能提高工作效率。

在工业 4.0 的生产和制造端，生产流程中的许多设备和机器都能接收和发送数字信息来驱动设备或机器的运行，同时还能根据该过程收集到的数据进行报告。在过去几十年里，计算机数控 (CNC) 机器都是利用 G 代码文件来对机床控制命令的自动化序列下达指令。增材制造 (AM) 进一步推动了数字化的发展，这项技术可以同时创建由数字信息包定义的一系列零件。与此同时，机器中嵌入的传感器和智能设备可以收集海量数据。

业内的一些产品生命周期管理 (PLM) 系统和协同平台，例如 Siemens Digital Industries Software 推出的 Teamcenter® 产品组合，[1] 它们可以处理企业资源规划 (ERP)、制造运营管理 (MOM) 和电子设计自动化 (EDA) 系统之间的数据集成，以及数字线程中不断创建的数字信息。此外，PLM 系统还可以将设计系统和制造系统链接在一起，让之前相互脱节的两项业务可以共享数字信息。

诸如 Siemens MindSphere 等数据收集系统可以帮助公司广泛收集由工业 4.0 和 IoT 生成的各类数字化数据。现在，借助数据收集系统中的内置分析功能，客户对其工艺流程有了更深入的了解。

在增材制造方面，Siemens Additive Manufacturing Network 可以提供针对按需生产提供设计咨询服务与功能，以及制造服务。这种分布式制造平台为公司带来了制造功能原型和连续生产零件的能力。



技术数据包

我们通常把数字线程中各种系统之间共享的数据集称为技术数据包 (TDP)。从设计到制造的整个流程中集成了大量工具和设备，因此对于系统间交换的 TDP，其规模和复杂性都在呈指数式增长。随着应用程序和系统的增加，为了支持这些系统间的互操作性，数字线程中的系统界面也变得愈发复杂。

尽管 PLM 系统能够协助管理零件的 TDP，但仍有必要在不同的系统之间构建数字界面，尤其是在多个不同的公司之间共享数据时。数字界面中互操作性与复杂性的提升，导致系统产生大量漏洞，非常容易受到网络安全攻击。IBM Security 报告显示，在 2016 年对制造系统的网络安全攻击中，有 74% 与尝试向数字界面注入攻击载体相关。

对制造系统的攻击可能涉及到知识产权 (IP) 盗用。例如，德国钢材与制造设备厂商蒂森克虏伯集团的设计 IP 曾在 2016 年被盗用。[2] 据 Manufacturing Business Technology 报道，21% 的制造商遭遇过网络攻击所致的 IP 损失。[3] 在其案例中，攻击者锁定的是对设备的物理性破坏。德国联邦信息安全局 (German Federal Office for Information Security, BSI) 就曾报道过攻击者让钢铁厂高锅炉过热的案例。[4] 此外，Stuxnet[5] 蠕虫对伊朗核计划的攻击也广为人知。除了盗用 IP 和实施物理性破坏，攻击者还有能力改变物理零件，L. D. Sturm 及其他研究人员对此进行过详细说明。[6] 据 Cybersecurity Ventures 预测，全球网络犯罪所产生的成本将从 2015 年的 3 万亿美元增加到 2021 年的 6 万亿美元。[7] 而在最近几年，勒索软件攻击导致了多起制造基地连续数天关停的事故。

“制造业已成为勒索软件的主要攻击对象。”

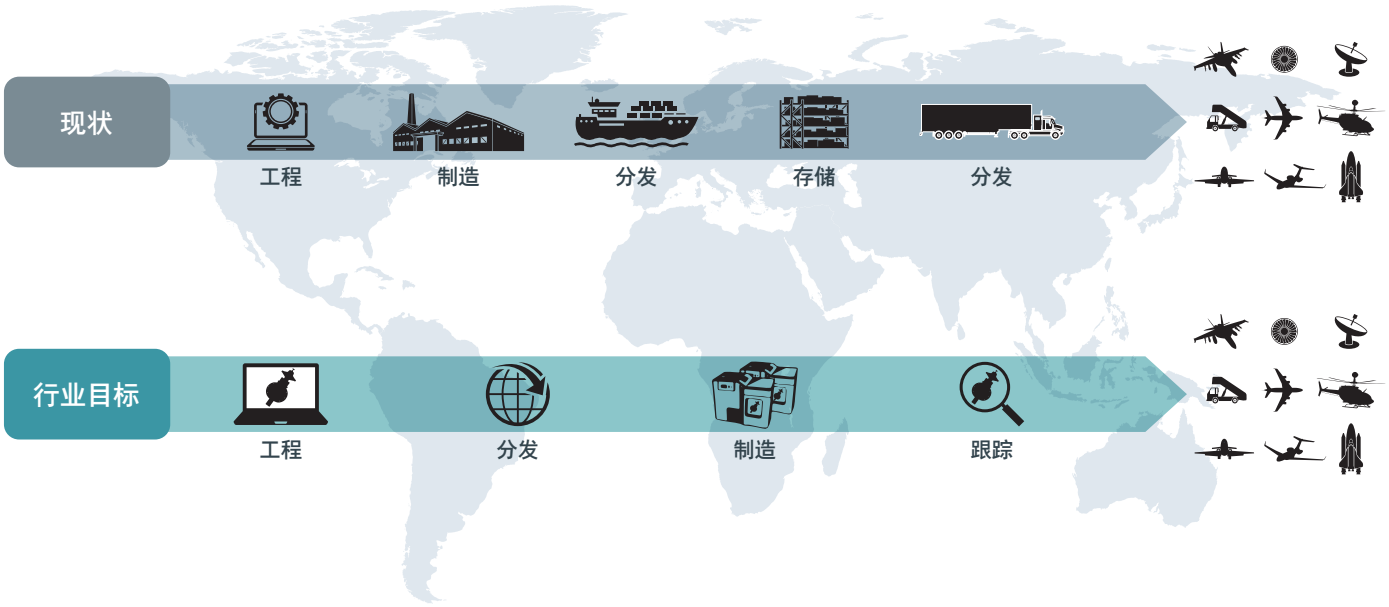
Carbon Black[8]

随着网络攻击的增加，以及制造系统和分布式供应链网络复杂性的提升，数字制造生态系统的安全维护工作也会愈发困难。据 Cybersecurity Ventures 预测，接下来 5 年（2017 年到 2021 年）内累计投入的资金将超过 1 万亿美元。[9] 此前，网络安全防御的重点在于保护设备的逻辑访问和物理访问，以及保护个别设备免受攻击。诚然，这些方式颇具价值，若执行得当确实能提供强有力的防御。 然而，考虑到数字制造线程的本质，位于不同物理位置且通常由不同实体拥有的设备与系统之间需要实现互操作性和协同。 这种情况下，就需要有一款更优秀的解决方案来专注于攻克核心挑战，也就是保护数字线程中的 TDP。

本白皮书介绍了一项新的技术，可以用来保护数字制造线程中的 TDP。Identify3D 应用程序套件可以保护从设计中心开始创建，到制造设备结束生产所产生的大量 TDP 的机密性与完整性，为数字制造提供 IP 保护、制造可重复性和可追溯性。通过将重心放在保护 TDP 上，客户可以确信自己的数据已作为不同系统间的 TDP 流而得到妥善保护，并且具有不同的拥有者和网络安全保护等级。

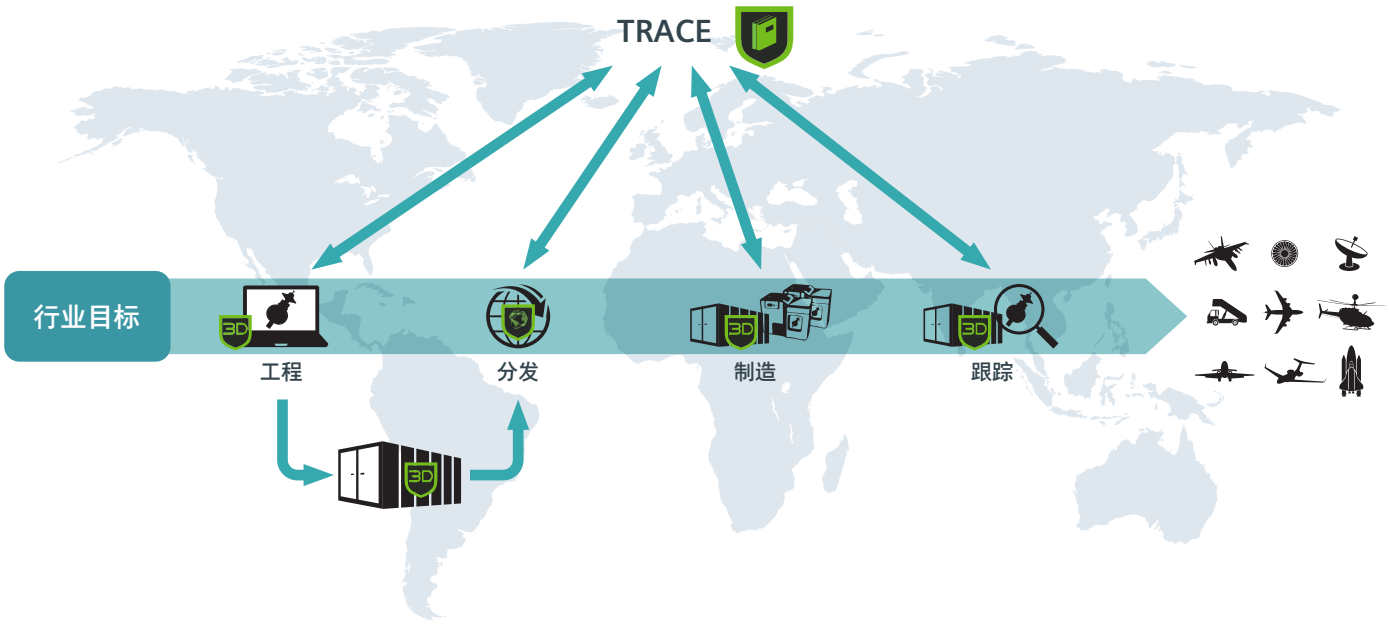
用于在数字线程中实施数据保护的全新解决方案

要实现制造数字化，我们需要重新审视我们的供应链。此前，供应链的重点在于使用包装盒和集装箱移动实物。而如今，这些实物要历经一段漫长且复杂的数字周期，而且在物理零件创建前就需要移动和管理数据。在数字线程中，我们可以使用对物理供应链的模拟。船运集装箱的出现颠覆了全球贸易，它的出现让货物得以轻松地从仓库运到港口，再通过铁路运输，接着装上大货车，最终运送到商铺。在数字线程中，TDP 必须在数字工作流中经历类似的旅程。安全的标准化物理容器颠覆了货物交换的方式，使物流系统之间的运输变得简单快捷且成本更低；同样地，数字容器也必须在数字线程中的不同应用程序之间实现无缝互操作性。



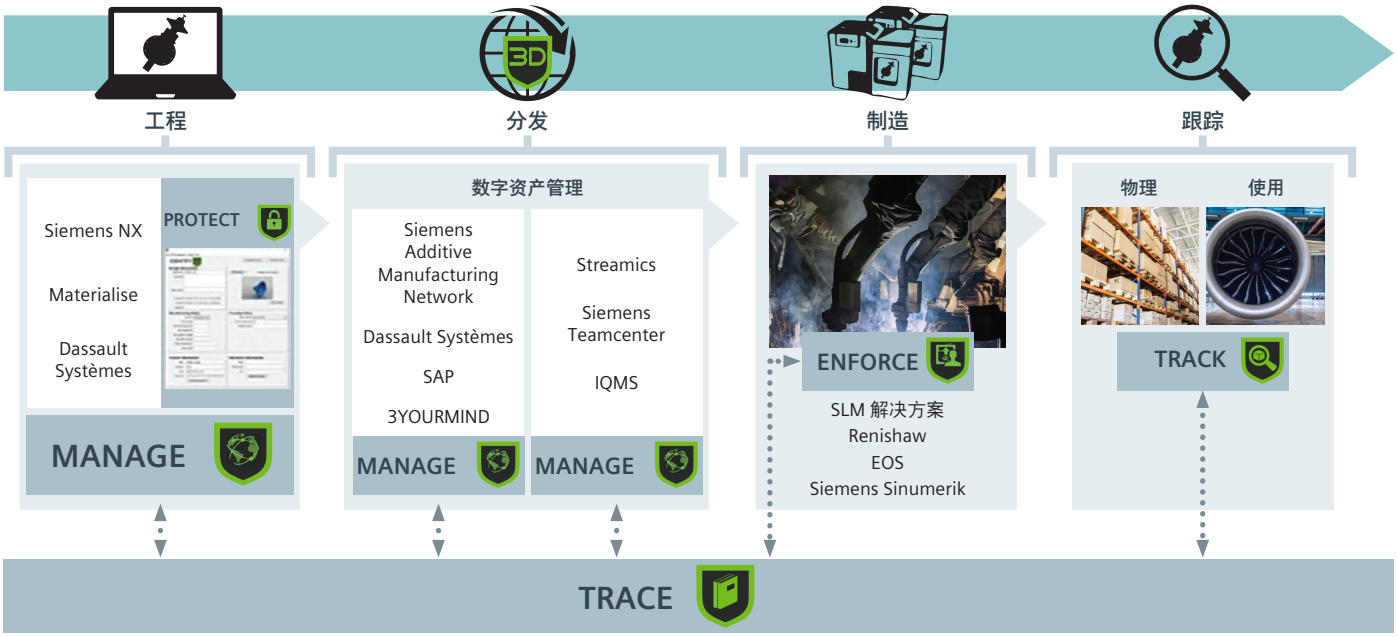
数字线程

Siemens-Identify3D 生态系统提供一种安全的数字容器来实现 TDP 在数字工作流中的移动。这款解决方案可在兼顾互操作性的同时全面保护 TDP。数字容器对存储资源库或安全传输方法也没有任何特殊要求。Identify3D Protect ™ 应用程序可以创建安全的容器，而 Identify3D Manage ™ 则会针对容器内 TDP 的使用创建分发和许可策略。通过与制造设备相集成，Identify3D Enforce ™ 能让应用程序和设备根据为容器定义的许可策略来访问 TDP。当安全容器在数字线程内移动时，Identify3D Trace ™ 会记录所有交易，同时 Identify3D Track ™ 会将物理零件 ID 链接到相应的数字化双胞胎。所有这些元素都会集成到西门子数字化工厂工具集中，从 CAD、CAM（计算机辅助制造）和增材制造软件应用程序，到机床控制器无所不包。



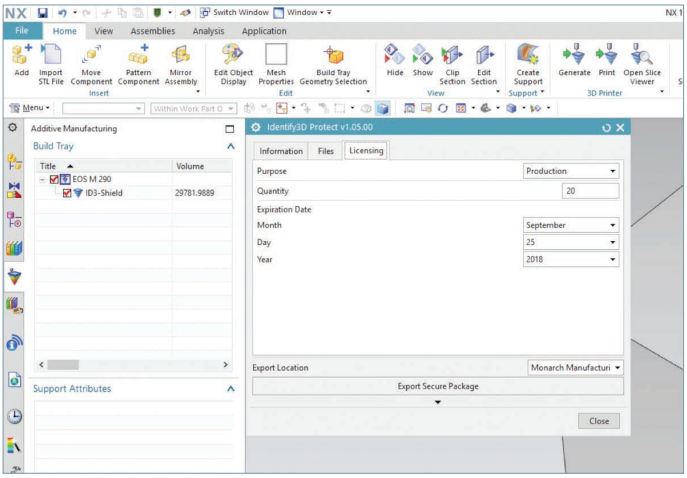
数字线程 - 解决方案

通过 Identify3D Protect，工业设计师可以将用于数字制造的 CAD/CAM 和 AM 文件存储在一个名为 Digital Supply Item (DSI) 的加密数字容器中，该容器采用数字签名并配有业务规则和生产规则。待数据包可供生产之后，整合在 TDP 中的所有数字文件都将安全地存储在 DSI 中。系统将使用生产规则和原始设计独有的其他规格为 DSI 创建许可。设计全面定稿之后，系统会对文件进行安全加密和数字签名；DSI 容器将传递到数字存储系统等待分发和生产；与此同时，数字许可也会传输到 Identify3D Protect。由于 DSI 容器已进行加密和数字签名，所以对 DSI 的数字存储和分发没有安全要求。



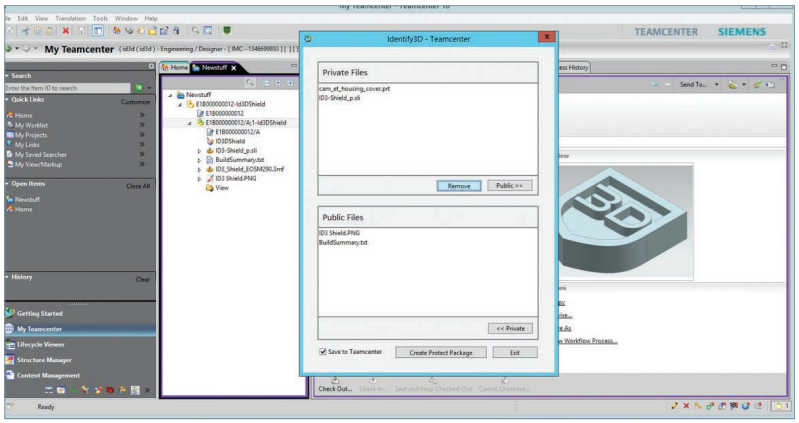
Identify3D 生态系统

通过将 Identify3D Protect 与 NX 直接集成，用户可以创建包含 CAD 文件、AM 构建文件或 CAM 后处理文件的加密 DSI。这种集成提供了无缝用户体验，系统会将所有数据包名称和文件描述自动拖入 Protect 模块。此外，下游 Identify3D Manage 的注册也可直接在 NX 内执行。



直接在 Siemens NX 中工作的 Identify3D Protect

Teamcenter 用户可以直接访问 Identify3D Protect 插件，因此他们可以在 Teamcenter 项目版本的文件内创建安全的 DSI 容器。创建 DSI 容器后，用户可以将它存储在 Teamcenter 中，也可以发送到下游资产存储系统，例如西门子制造执行系统 (MES)。



直接在 Teamcenter 中工作的 Identify3D Protect

Identify3D Manage 从 Identify3D Protect ™ 接收到许可时，便会创建一个新的订单，以便用户进行安全可靠的数字分发。用户可以将 DSI 的分发和制造权分配给任何数字经销商或数字制造商。本质上，我们可以根据用户、系统所有者或与系统相关的任何数字财产，安全地控制任何系统内的 DSI 可操作性。分发订单时，Identify3D Manage ™ 可以对被许可人可生产的零件施加限制。系统将针对工程、分发和制造过程以定制形式提供 Identify3D Manage 应用程序。

例如，Siemens Additive Manufacturing Network 将在分发模式中运行。Identify3D Manage 的实例将在网络中运行，在零件作为生产订单进入以及进到制造环节时，对其实施管理。这种方式可以确保在执行增材制造工作流的这些步骤期间，客户的数据能在 Siemens Additive Manufacturing Network 中得到安全管理。

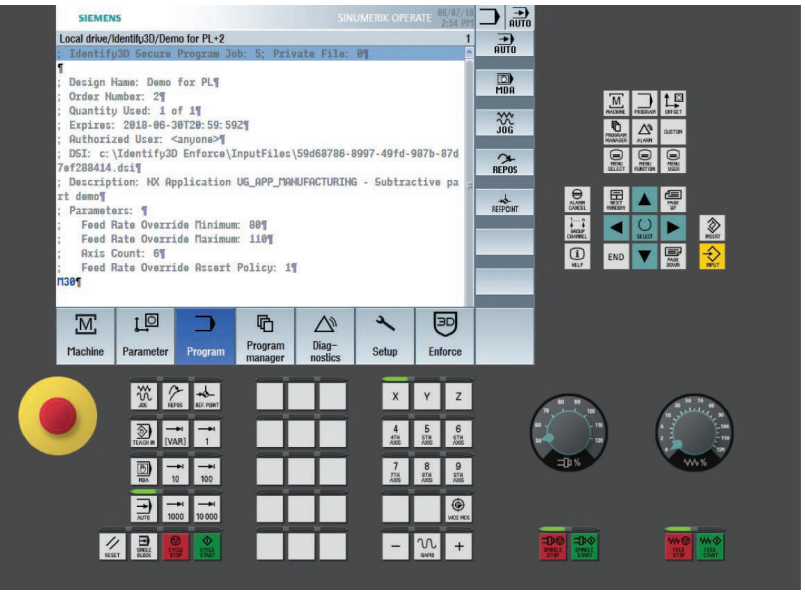
生产零件所需的特定制造机器可以按照制造、建模、甚至是单机进行指定。用于控制零件制造的任何数字参数都将被限制在某个范围内或限制为某个值。许可还可规定与设备相关、可确保一致的重复生产能力的任何资格或认证。Siemens-Identify3D 生态系统可对能够按零件生产的制造系统施加完全控制，从而确保 IP 拥有者获得始终如一的质量。

Identify3D 许可策略支持严格的身份管理控制。这样，客户就可以要求只有单独定义的许可用户，或者通过组、角色或认证状态定义的许可用户才能生产零件。依据这项策略，不仅可以让客户确信数字线程中的系统用户都通过了本地身份管理系统的身份验证，而且客户还能要求拥有适当资格的特定用户在已定义制造系统上访问并使用 DSI 中的受保护文件。

完成数字分发并做好零件投产准备后，Identify3D Manage 将为内嵌了 Identify3D Enforce 应用程序的制造设备生成许可，以供生产零件时使用。Identify3D Enforce 会验证许可、机器设置、用户及 DSI 的完整性，以确保生产期间设计的安全性与完整性。只有完成全面验证后，Identify3D Enforce 才会解密 DSI 容器，并将许可的文件提供给机床控制器用于生产。

在制造设备生产零件期间，Identify3D Enforce 会持续监控流程，确保所有受保护的设置和参数始终在许可的值和范围之内。此外，Identify3D Enforce 还会跟踪设备生产的零件总数，确保未超过许可设备生产的最大数量。

从 2018 年 6 月开始，我们将 Identify3D Enforce 集成到了西门子 SINUMERIK 840D sl CNC 控制器当中，允许利用加密 G 代码文件加载安全的 DSI 容器，以实现顺畅的用户体验。



集成到西门子 SINUMERIK 840D sl 中的 Identify3D Enforce

NIST SP 800-82 publication10 和 IEC 62443/ISA-99 标准中概述了制造网络安全的最佳实践。[11] 一般来说，其中会涉及指定生产场地中易受攻击的重要设备、基于所需保护等级分配安全等级，以及创建隔离区域。此外，适用于单个系统的标准网络安全实践也同样适用，比如让软件修补程序保持最新状态、创建审计线索、限制访问、实施适当的防病毒和文件一致性检查，以及禁用不使用的端口。对系统进行持续监控也十分重要，尤其是在入侵可以被检测到的情况下。

对静态数据进行加密也是推荐的最佳实践。加密确实是确保数据安全非常重要的一个方面，但为了保留数字线程中各个系统之间的互操作性，数据必须在系统之间的界面上进行解密，而这就会引入漏洞点。Identify3D 通过允许 DSI 中的加密数据在应用程序之间传递，很好地解决了这个问题。只有当内嵌在制造设备中的 Identify3D Enforce 应用程序访问加密数据时，加密数据才会解密为纯文本格式。

过去加密系统所存在的一个最复杂的问题就是管理和保护必要的加密密钥，而发生泄密的一个主要原因就是对密钥的保护不力。行业中有多种方法可以用来保护加密密钥，其中包括硬件安全模块 (HSM)、智能卡和信任平台模块 (TPM)。考虑到客户对安全等级的要求各有不同，因此 Identify3D 支持任意行业标准的加密密钥保护，包括使用联邦信息处理标准 (FIPS) 或通用标准认证设备。每一个利用加密密钥的 Identify3D 应用程序都将可以访问受保护硬件来源提供的密钥。

实施 Identify3D 生态系统并不意味着不必遵循制造网络安全方面的最佳实践；相反，遵循这些最佳实践将有助于增强 Identify3D 保护等级。实施最佳实践后，最薄弱的点就变成了互操作性要求以及与内部人员相关的威胁。Identify3D 在兼顾加密的同时保留了互操作性，通过在 DSI 中加密 TDP 来防止内部人员在数字线程中的任意位置访问 TDP。Identify3D 应用程序套件将重点直接放在 TDP 的保护上，目的就是为了确保 TDP 在整个数字线程中的机密性与完整性。

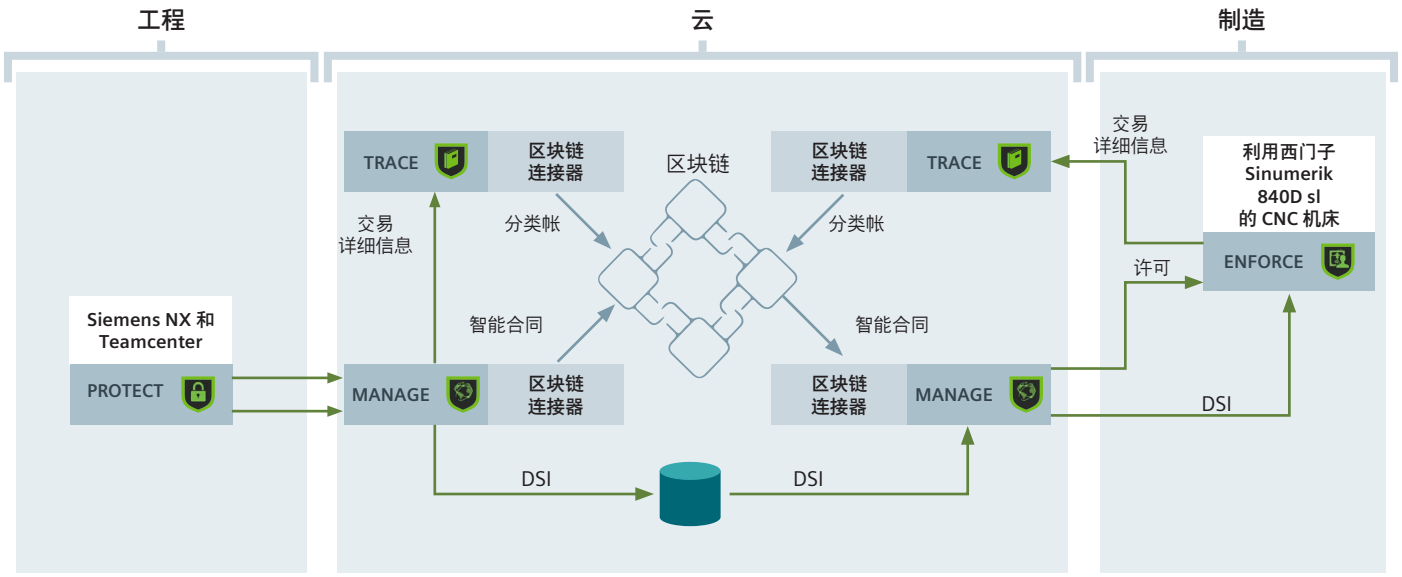
除了在数字线程中保护 IP 安全并保证质量外，Identify3D 技术还会安全地存储该 IP 的所有操作和交易。Identify3D Trace 会存储涉及 DSI 的每一次数字交易的记录。这样，针对每个 TDP 的数字制造和分发，都会保留一份审核记录。存储在交易中的所有数据都会加密，而且 IP 所有者可自行决定是否允许参与 TDP 数字制造的所有实体访问这类加密的数据。制造物理零件后，Identify3D Track 会记录零件的识别号并将其添加到 Identify3D Trace 分类帐中，以便在数字线程和物理线程之间建立关联。此外，由 Identify3D Trace 存储的这些安全数据会提供给 Siemens MindSphere 系统或其他数字数据收集系统，以便于保留。

区块链

区块链技术能以去中心化的开放数据资源库取代集中的专用数据库。在区块链内，每一个参与节点都可以添加到正在运行且始终更新的共享分类帐中。共享分类帐拥有强大的加密完整性保护，可保留特定区块链中交易的完整记录历史。此外，每一个节点可就任何交易的真伪进行投票并拒绝欺骗性交易。区块链的去中心化本质意味着，没有任何一家单独的公司能够拥有分类帐中记录之数据的所有权，或对其造成不当影响。

由于每一个 Identify3D 应用程序都在独立节点上执行，因此在供应链区块链中实施 Identify3D 生态系统十分直接，不需要对核心 Identify3D 技术进行任何更改。有多种实施可行，具体取决于所使用的特定区块链技术。对于诸如 Hyperledger Fabric 这类允许数字合同的较复杂区块链，由 Identify3D 创建的整个数字许可将存储在区块链中，而且可利用数字合同进行许可。对于简单一些的实施，可将许可的数字签名哈希记录存储在区块链上。无论是哪种情况，许可交易的记录都会由区块链保留。如果整个许可内嵌在区块链中，则区块链本身会作为一种机制，用于在不同节点之间传输许可。许可中的所有机密信息都会采用许可加密密钥进行加密，以保持交易的完整性，同时维持 IP 的保密性。

Identify3D 增强了供应链区块链，它会将数字化双胞胎的记录添加到使用数字制造技术所创建的每一个物理零件中。这样，最终装配的产品将具有包括制造运营、数字设计，以及完整产品中所含 IP 的完整记录。



Identify3D 与区块链集成的示例

软件 / 硬件连接

现在，通过将 Identify3D 解决方案集成到西门子数字套件中，用户能够在从创建到制造的整个过程中保护其 IP 的机密性与完整性。

例如，航空航天制造商可能对 20 种 CNC 制造的替换零件有快速周转的需求。由于他们已经完成零件设计并有了定稿，因此 TDP 会作为项目版本存储在 Teamcenter 中。用户可以选择 TDP 并使用 Identify3D Protect 创建 DSI，同时限制为只有符合标准的机器才能制造这些零件。接下来，航空航天制造商会通过 Identify3D Manage for Engineering 授权合同制造商生产这 20 种零件。

分包商收到授权后，他们判断必须借助另一个分包商才能满足生产量需求。于是，他们使用 Identify3D Manage for Distribution 授权自己的车间制造 12 种零件，同时授权其他分包商制造另外 8 种零件。

而合同制造商将会收到在自己车间运行 Identify3D Manage for Manufacturing 的授权，并且能够选择授权三台有资格生产零件的 CNC 机床。在这种情况下，合同制造商将会指派每一台机器制造四种零件。在每台机器上运行 Identify3D Enforce 的西门子 SINUMERIK 840D sl 控制器将接收到包含特定于零件的 G 代码的 DSI 并创建任务；之后，鉴于每一台机器都具有合格的认证，操作员便能选择任务并只生产四种零件。

流程完毕后，航空航天制造商就能查看订单成功完成的记录，包括通过 Identify3D Trace（可以在 Siemens MindSphere）所使用的每一台机器的报告。航空航天制造商将会看到合同制造商使用的分包商，并能查看分包商使用的两台 CNC 机床的报告。

结论

工业 4.0 颠覆了企业的制造方式。与其他行业一样，制造业正在经历资产和流程的数字化转型。因此从某种程度上讲，未来已在眼前。然而，要想真正把握数字化带来的优势，企业需要在实现数字供应链转型的过程中，管理、控制并跟踪海量数据。

只有按照严格控制的安全流程，在恰当的时间将适当的数据传递到正确的机器中，才能实现去中心化的制造模式，从而获得在所需的时间和地点按需制造的能力。

无论是数字供应链还是物理供应链，其完整性对于阻止盗版泛滥、恶意修改、质量不佳或未经认证的零件流向市场都至关重要。Identify3D 提供的各项技术可以保护静态数据、通过许可管理数据流，以及保留不可更改的移动记录，但这些都需要经过较长的过程，才能为那些新的制造业务模式的安全部署提供支持。

参考信息

1. https://www.plm.automation.siemens.com/en/plm/digital-manufacturing.shtml
2. https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW
3. https://www.mbtmag.com/article/2017/03/top-cybersecurity-threats-manufacturing-2017
4. http://www.bbc.com/news/technology-30575104
5. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
6. Sturm、L.C. 等，“增材制造系统中的‘网络-物理’漏洞：通过人类主体对 .STL 文件进行攻击的案例分析 (Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects)”。*Journal of Manufacturing Systems* 第 44 卷，第 1 部分：2017 年 7 月，第 154-164 页。
7. https://www.prnewswire.com/news-releases/cybercrime-damages-are-predicted-to-cost-the-world-6-trillion-annually-by-2021-300540158.html
8. https://www.infosecurity-magazine.com/news/nonmalware-attacks-on-the-rise
9. https://www.infosecurity-magazine.com/news/annual-cybercrime-costs-double-6
10. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
11. https://www.isa.org/isa99

Siemens Digital Industries Software

总部
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

美洲
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

欧洲
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

亚太地区
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

关于 Siemens Digital Industries Software

Siemens Digital Industries Software 是 Siemens Digital Industries 的一个业务部门，其致力于推动行业数字化转型，为制造商实现创新创造新机遇，可谓是全球领先的软件解决方案供应商。总部位于美国得克萨斯州普莱诺市，在全球拥有超过 140,000 个客户，并与所有规模的企业协同工作，帮助他们转变将想法变成现实的方式、产品实现方式以及使用和了解运行中产品和资产的方式。有关产品和服务的详细信息，请访问 siemens.com/plm。

siemens.com.cn/plm

71790-81625-C7-ZH 2/20 LOC