

筑牢工业信息安全防线

文 / Nicolas Bennerscheid, Lars StephanBüldt, Sebastian Dännart

安联 2023 年的风险报告分析称，除了业务中断之外，网络风险是全球企业面临的重大风险。因此，需要通过做好基础网络安全监测与防御，避免企业受到网络攻击的可能性。

对于流程工业的任何一家公司来说，一旦受到网络攻击，如果不及时采取措施将会遭到致命打击。2023 年《安联风险晴雨表》显示，网络风险如 IT 中断、勒索软件攻击或数据泄露，一直被认为是全球企业面临的重大风险。

网络攻击到底是如何实施的？

随着信息安全技术的高速发展，信息安全技术的全球性、互联性、信息资源和数据共享性等特点日益突出。使其极易受到各种类型的网络攻击，网络攻击的不可预测性、危害的连锁扩散性，大大威胁到信息安全的发展。很多网络攻击都是从监视和收集信息开始的，比如网络“钓鱼”或者其他社交工程手段。当获取目标的信息之后，就会开始初始攻击。如果网络“钓鱼”攻击成功，攻击者就可以方便地访问目标系统，然后利用获取的访问数据实施欺诈等行为。

信息安全管理规范

例如石油天然气、化工和制药等许多行业，都制定了严格的敏感信息保护规定，包括功能安全参数和一些相关数据。《德国信息技术安全法》和《事故条例》规定了保护设施免受网络攻击和检测网络攻击的要求，关键信



大多数黑客攻击都是从网络钓鱼攻击开始的

息基础设施和具有特殊公共利益的公司将承担更多的责任，关键信息基础设施运营商必须采取技术和组织措施，以防止其信息技术系统、组件或流程的可用性、完整性、可靠性和保密性遭到破坏。

数据泄露对安全生产的影响

业务流程数字化经常被认为是企业利用新兴技术更新现有流程并加强竞争基础的最有效方式之一。然而随之也带来了一系列问题，比如工厂设备的一些关键数据需要注意传输安全。信息安全的保护目标与职业安全和事故预防也变得更加重要，在数据采集、传输和处理过程中，需要采取有效的措施保障数据的安全性和隐私性，防止数据泄露和滥用。

因为当工业企业的信息比如工艺生产设备的一些功能参数遭受破坏、更改、泄露后，工业生产设备、控制系统、信息系统将不能可靠正常运行，

工业生产和业务的连续性也得不到保障。当安全参数（如温度或压力限值）泄露后，可以提供工厂运行状态相关信息，这可能会增加攻击者的成功机会，从而导致运行完整性受损和安全风险增加，甚至会发生安全事故。

假设有一家处理危险化学品的化工厂，其处理、存储和处置这些化学品的整个工艺流程数据，以及为保护环境而采取的安全措施等信息落入了不法分子之手，不管是数据泄漏或未经授权可以成功访问系统，都有可能导致工厂处于不安全状态。为了避免这种情况发生，必须采取必要的措施来保护这些机密数据。

加密过程数据通常包含有关监测系统、警报和应急计划等安全防范措施信息。恶意攻击者可以利用这一发现来操纵或绕过安全系统，例如通过更改警报阈值或操纵传感器配置来延迟停机。如果阀门意外打开或发生故障没有被正确记录，这可能导致危险化学品的意外释放，进而造成环境污染，并对人类和动物造成危害。

这种方法，即有针对性地关闭工业应急系统，特别是控制系统，是现代恶意软件包的主要功能之一，如“Industroyer2”和“Pipedream”/“Inconroler”，前者于 2022 年在乌克兰使用，目的是破坏供应网络，后者是在美国发现的一个来源不明的恶意软件包。

目前有些恶意软件包就是专门攻击工控系统，比如美国网络安全和基

本文作者 Nicolas Bennerscheid 和 Lars StephanBüldt 供职于 TUEG - Schillings 公司，Sebastian Dännart 供职于 Infodas 公司。

基础设施安全局（CISA）等机构已确定“Incontroller/PipeDream”恶意软件对液化天然气和电力供应商等能源机构和组织构成严重威胁。攻击者可使用该恶意软件对目标工业环境进行侦察，并控制 PLC，实施可能导致工厂中断、安全故障和潜在物理灾难的破坏活动。

信息保护影响评估

为了评估哪些信息和通信流值得保护，首先必须明确了解或公布这些信息和通信流会产生什么影响。所谓的保护需要评估有助于确定必要的保护措施水平。

首先确定相关信息。这项工作听起来可能有些琐碎，但实际上需要对涉及的系统和业务流程进行深入分析，并需要专业部门的参与。因此，拥有良好的系统文档和成熟的业务流程管理是非常重要的基础。此外，对过程安全和功能安全概念的全面理解是必要的，特别是在确定过程工程系统中的安全参数的保护要求时。在某些情况下，相关的行业标准和法规已经明确规定了相关要求。如果已知相关数据和信息，就可以评估某个安全目标的损失所造成的影响。同样这里也需要专业部门，因为只有通过他们才能进行有效地影响评估（业务影响分析）。

保护相关系统的机密性

为了确定适当的保护措施，必须区分需要保护的数据和信息的状态：存储在硬盘或其他数据载体上的信息和参数，即“静态数据”；正在传输或通信中的数据和参数，即“动态数据”。

在保护“静态数据”的保密性方面，重点是通过授予权限和选择加密单个信息或整个硬盘来保护访问。这里的基础是组织措施中描述的授权概念。在“动态数据”传输的情况下，通信保护是重中之重，如果信息传输是必要的和有计划的，也可以对数据和信

息进行加密。此外，还可以通过安全网关和数据二极管自动限制特定的内容、数据类型或通信方向。在工业应用中，这类过滤还可实现控制信号或参数的非加密。基础设施措施也可在信息保密方面发挥作用，例如在相关区域安装镜面窗以实现视觉和窃听保护，以及用于访问保护安全系统，防止未经授权访问隔离系统。这些措施的必要强度取决于个别数据和信息的保护要求，应根据风险确定优先次序。

组织措施保护信息安全

通常情况下，由于一般条件的限制，技术措施可能不可行，或者会在不可持续的程度上阻碍业务流程的顺利进行。虽然技术措施能提供更可靠的保护，但在这种情况下也可以采取组织措施。组织措施主要包括描述安全措施和其实施的概念，以及规定相关利益方遵守某些行为的准则和指导方针。最基本的指导方针也是设计后续技术措施所必需的，这涉及信息的分类和分级以及具体如何

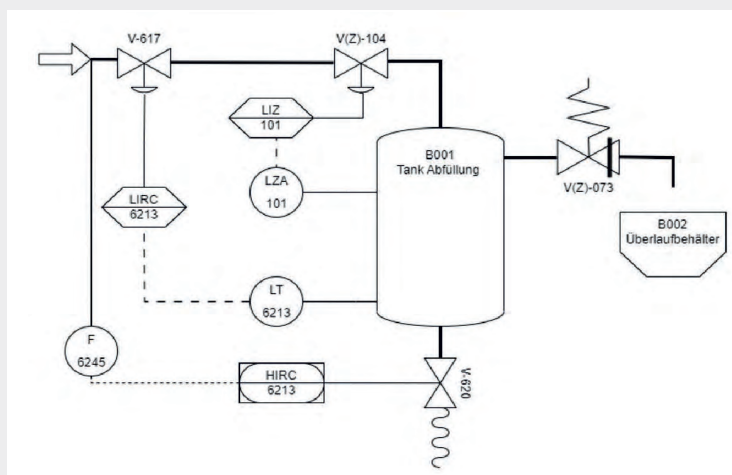
储罐实例

用流程工业普遍需要使用的储存设备储罐，这样一个简单而具体的例子，来展示信息失密造成的危害。

B001 储罐用于储存一些危险介质（如液体），并通过测量底部压力 LT6213 来监测其液面水平高度。当液面高度超过上限值时，B001 储罐入口的阀门 V-617 将自动关闭。此外，B001 中的临界液位由音叉液位开关 LZA101 监测。当液位达到临界水平时，入口处的附加安全阀 V(Z)-104 会关闭。此外，还有一个机械过量加注保护装置，当 B001 储罐完全加满时，允许液体溢流到 B002 储罐。储罐可通过阀门 V-620 关闭的软管排空，该阀门可在入口关闭的情况下通过现场

手动操作打开。

为什么有关系统和组件配置的信息需要严格保密呢？比如 B001 储罐存储了很多危险液体，然而当攻击者通过蓄意破坏或者改变储罐一些关键参数，这时就会造成储罐泄漏危险液体。需要注意的是，目前不仅会受到物理攻击，网络信息攻击也能带来风险。如果攻击者知道地面压力传感器 LT6213 关闭阀门 V-617 的限值，则可以通过改变相关参数，这样能破坏储罐，造成危险发生。特别是在传感器联网，参数存储在数字系统中的现代系统中，这些参数更容易被读取，工业信息安全易受攻击，工业安全生产必须得到适当保护。



这个储罐用于存放周围部件所需的物料

（下转第 25 页）

本安以太网), 这个缩写全称是 Two-Wire Intrinsically Safe Ethernet 即 IEC TS 60079-47 国际技术规范。2-WISE 为本质安全的 Ethernet-APL 制定了严格的规范, 包括组件的技术特性以及网络的设计、安装和文档编制。

Ethernet-APL 是基于 10BASE-T1L 单对以太网 (SPE) 的一种增强型物理层, 只使用两根线缆即可完成对数据和电力的传输, 而且速度很快。因此所需空间更少, 这使得在狭窄的机器中的安装更加容易。

与化学工业同行

Lapp 缆普电缆公司 (以下简称“缆普电缆”) 是单对以太网领域的先驱之一, 并通过与一些标准委员会在 Ethernet-APL 方面进行了合作。作为可以提供综合解决方案、品牌化线缆产品以及连接技术的全球领先供应商, 缆普电缆专注于电缆和连接技术领域, 在 2023 年 SPS 展会上展示了两款用于 Ethernet-APL 的电缆产品: Etherline T1L Y FC 1×2×18/1 AWG 和 Etherline T1L Y 1×2×18/7 AWG。两款产品均符合 ISO/IEC 11801 和 EN 50173 标准, 以及 IEC-

61156-13CD 的传输特性要求, 并获得了 UL 认证, 因此适用于在北美地区使用, 这对于出口型企业来说是一个巨大的优势。这两款电缆产品适用于长达 1 000 m 的距离, 具有阻燃、抗紫外线老化和耐油等优点。

另外这两款产品均可通过数据线供电 (Power over Dataline, PoDL), 功率可达 92 W。两者均采用缆普电缆开发的 Fast-Connect 设计, 因此易于剥离和安装。唯一的区别在于 Etherline T1L Y FC 1×2×18/1 AWG 采用了固定安装的实心导线, 而 Etherline T1L Y 1×2×18/7 AWG 具有 7 股导线结构, 适合于偶尔移动的应用。为确保线缆的实用性, 它们根据德国一家领先的化学企业的要求, 进行了开发和共同测试。

自动化为流程工业带来更多可能性

从外观上看, 这两款电缆与传统的以太网或 Profinet 电缆有所不同, 因为它们都采用蓝色护套, 这是因为 Ethernet-APL 协议规定了电缆使用蓝色护套。内部也与传统的 SPE 电缆有所不同, 导线直径、双绞线的绞



Ethernet-APL 规定了电缆使用蓝色护套

合、绝缘层的厚度等参数都需要进行调整, 以满足对内在爆炸防护的要求。缆普电缆的工业通信产品经理 Christian Illenseer 说: “把所有这些参数调整到一个和谐的状态下, 以满足 Ethernet-APL 的要求, 这是一门艺术。”

当涉及尽可能多的不同应用场景时, 缆普电缆这两款产品优劣自然分明, 不过也具有通用性, 例如得益于获得过很多认证, 这两款电缆可以广泛应用于开放式电缆平台中。流程工业中的生产商和设备商现在都应该重视 Ethernet-APL, Christian Illenseer 建议道: “Ethernet-APL 是现场级的升级, 为流程工业生产带来了更高性能和更多的数字化机会, 同时确保了最大的安全性。”

(上接第 23 页)

处理。在此基础上, 一个复杂的授权概念定义了谁可以访问、更改或删除哪些数据和信息。如果员工自愿或意外地泄露了信息, 即使有再好的技术措施和最佳的组织框架条件也无济于事。因此, 针对特定目标群体的宣传和增强所有员工的安全意识至关重要, 这不仅包括对数据和信息相关性的认识, 还包括为什么遵守组织措施能保证实际保护。

反复开展培训和宣传活动有助于形成一种“安全习惯”, 让员工能够在日常工作中直观地掌握与安全相关的措施, 从而为保护数据和信息的机密性做出积极贡献。

注重生产安全, 不仅为了合规

在工艺设备中负责关键安全参数和数据的人员必须意识到, 保密对工厂的运营安全至关重要。这不仅是为了遵守法律法规, 更是为了提高安全性和保障性。合规是安全的底线, 安全是合规的目标。企业若只满足合规要求, 就一定会忽略关键的漏洞, 会使“只追求合规”的公司面临着他们所不知道的漏洞风险, 比如当工厂一些关键生产数据被竞争对手掌握时, 会导致业务被抢走, 甚至有时候还会造成人身安全。因此, 安全和合规是相辅相成的, 合规是基础, 是核心,

合规必定是安全的主线, 安全也必定是基于合规的安全。

幸好目前, 我们有办法最大限度地降低这些风险并减轻其影响。通过确保基本的安全措施并对自身的流程和系统进行单独分析, 可以获得基本的保护, 从而能够在节约资源的同时专注于公司的核心业务。根据公司的情况, 可以选择在内部或外部获得支持进行分析。这样, 就能有针对性地制定计划和措施, 以满足每个公司的不同需求, 从而为公司的成功做出经济贡献。此外, 还能够满足相关法律要求。