CCID 赛迪智库 译丛

2017 年 2 月 13 日　　第 5 期　　总第 290 期

工业物联网安全框架

【译者按】当前，融合了信息技术与运行技术的工业物联网系统正在迅猛发展，其安全问题也引发业界的高度关注。2016 年 9 月，工业互联网联盟发布了《工业物联网安全框架》，从工业物联网的系统特征、构成要素、安全评估以及运行保障等方面，阐述了技术、架构、人员、机制、战略等构成要素对工业物联网系统安全的影响。在此基础之上，报告对工业物联网重要构件——端点的安全问题进行了深度分析，以期为设计部署和应用工业物联网的机构提供指导。赛迪智库网络空间研究所对该报告进行了编译，希望为我国相关决策部门提供参考。

【关键词】 工业物联网　运行技术　系统特征　安全框架

一、工业物联网的本质特征

（一）历史成因

工业物联网（IIoT）系统连接和集成了不同类型的控制系统、传感器、企业系统、业务流程以及分析和人员，增加了系统的多样性和规模。

传统上，可靠的工业系统的安全性依赖于对易损部件的物理隔离和网络隔离以及对关键控制系统的隐藏设计和访问限制。由于潜在的人为错误或误操作都来自于对系统的直接接触，因此人们主要关注的是系统的安全性和可靠性，而这些风险可通过优化设计、分析和审查及全面的测试和训练加以避免和缓解。随着控制系统、商业系统和互联网的不断融合，最初设计为隔离状态的系统现在暴露在日益复杂的攻击环境中，对工业物联网系统的成功攻击可能导致环境破坏或人身伤亡，严重程度甚至堪比迄今为止最严重的工业事故。

在工业物联网系统中，各种系统特性必须相辅相成，以实现整体系统的可靠性。如图 1 所示，对信息技术（IT）和运行技术（OT）而言，弹性对后者更为重要，而安全性则对前者更为关键。与传统信息技术环境相比，相关机构应更加重视工业物联网的安全性和弹性。工业物联网系统包含中间设备并涉及多个机构的数据流，需要比通信加密等更为复杂的安全手段。

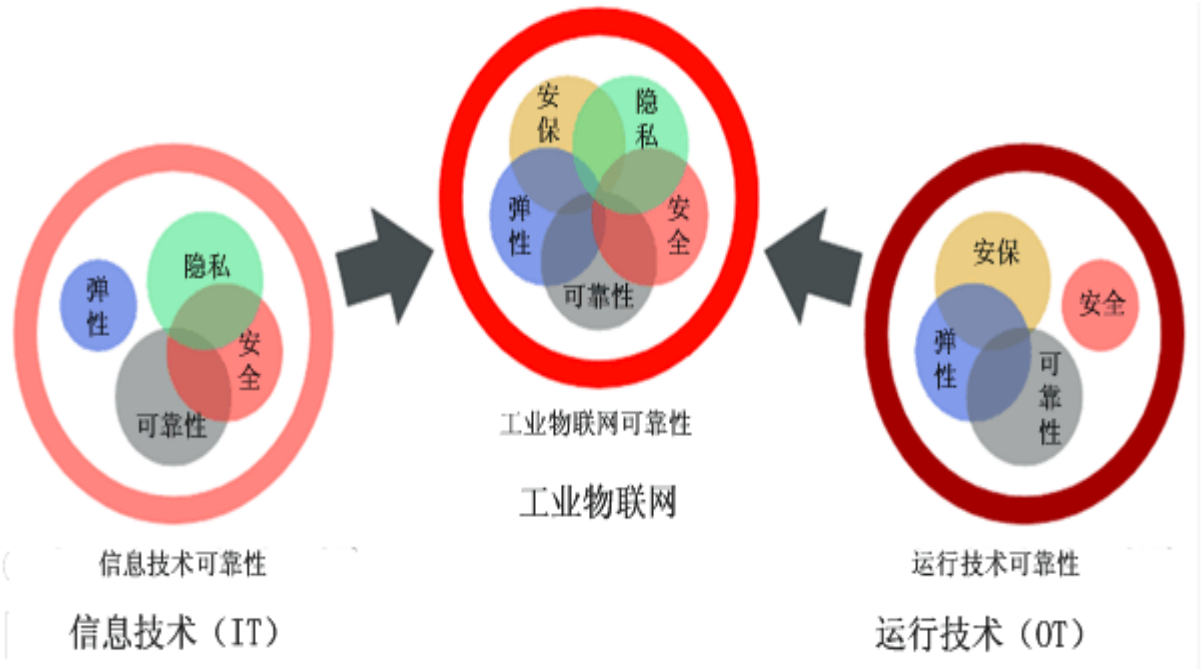

图 1　信息技术可靠性与运行技术可靠性的融合

（二）实现系统可靠性的五大关键

工业物联网系统呈现出端到端的特性，是其各种组件的性质和相互作用的结果。安保、安全、可靠性、弹性和隐私这五大特性是影响人们是否授权部署工业物联网的主要考虑因素。其他特性，如可扩展性、可用性、可维护性、可移植性或可组合性虽然重要，但却不是保证物联网可靠性的“关键”特性。

1、安保

安保是指保护系统免受意外或未经授权的访问、更改或破坏。任何工业物联网系统都不可能在各种环境下均能保持安全，因此必须明确说明物联网所处的特定环境和人们对物联网的安

全要求。在传统的运行技术系统中，人们最关注可用性（Availability），其次是完整性（Integrity），而保密性（Confidentiality）通常是最后考虑的因素。其中，可用性是指授权用户根据指令可及时和可靠地访问和使用信息的属性；完整性是可确保信息不会被不当地修改或破坏的属性；保密性是指不向未经授权的个人、实体或流程提供或披露信息的属性。

2、安全

安全是一种系统运行状态，在此状态下，不会因财产损失或环境破坏，对人身健康造成直接或间接伤害。传统的运行技术和安全评估技术侧重于物理项目和流程评估，并将根据经验得出的组件故障概率纳入总体系统风险。识别危险的风险分析旨在预防错误操作，并提高系统对意外事件的抵御能力。许多用于生产关键安全软件的工具、技术同样可以识别、消除和减少潜在安全漏洞。许多安全规程和指导文件要求在关键安全系统中使用的软件需要进行严格的检验和使用验证，严格的软件开发惯例可以帮助开发人员识别和消除潜在的安全问题和安全漏洞。

3、可靠性

可靠性是系统或组件在规定的条件和特定的时间段内实现其所需功能的能力。可靠性是规划可用性的实际可用性部分，受计划维护、更新、修复和备份的影响。而保证可靠性需要详细了

解运行环境、系统组成及其设计和预置条件，以判断失效的可能性，同时需要了解各要素的参数、配置设定和物理属性，并且还需确定是否实施上述规划值的验证活动。在可靠性保障实例中，还需了解整个系统及其组件正常运行时间要求和平均故障时间分布情况。为提高系统的可靠性，应充分考虑攻击者能够影响可靠性的哪些方面，并有针对性的进行系统和安全设计，以应对此类攻击。

4、弹性

弹性指系统的应急特性：即系统能规避、吸收和管理动态的敌对环境，以及在出现不利苗头时，重组系统运行能力。通过系统设计、故障隔离，来实现系统的弹性。同时系统软件还必须具备相关能力，来针对特定位置或网络区段可能存在的不同薄弱环节。

5、隐私

隐私是个人或团体的一项权利，即控制或影响与他们自身相关的何种信息可以被何人搜集、处理、拥有以及可以向何人透露。保障隐私取决于利益相关者是否希望或法律是否要求保护或控制相关信息以防用于某种用途，同时必须符合最新的法规和标准规定。工业系统与包含敏感数据的其他系统互连，可能会增大隐私风险。

（三）影响工业物联网的安全因素

传统上，信息技术和运行技术系统的安全性一直分别单独评估，但工业物联网系统不是信息技术和运行技术的简单融合。可靠的工业物联网系统要求其安全功能在信息技术和运行技术两个方面进行端到端评估。信息技术和运行技术安全性的整合需要了解两者之间的差异及各自评估和保护系统的方法。

1、信息技术和运行技术的融合

信息技术和运行技术的融合涉及各自关键系统特性的复杂整合，系统的整合改变了信息技术和运行技术的安全模式。如因不当的安全措施导致存储在信息技术系统中的控制信息未经授权的修改，则依赖这些数据的运行技术系统就可能失效。信息技术和运行技术的融合需要不同的重点和态度，而这两种技术对关键系统特征及其保证方式有着不同的考虑，必须综合考虑工业物联网系统执行的各种功能。

2、信息技术和运行技术的安全演变

信息技术系统中的风险评估取决于成功攻击的可能性和所造成的损害，但这种损害通常涉及金钱或声誉，很少考虑其他后果。在运行技术中常见的攻击类型（例如物理攻击）并非决策考虑的内容，且网络元素亦不考虑工业协议。当前，消费者正在向信息技术网络添加新的设备（例如灯泡或电视），使用工业系统

协议控制家用电器。与此同时，运行技术系统亦增加了更多的信息技术组件，特别是运行设备管理软件的控制台。因此，即使没有连接到网络的控制系统同样面临着信息技术的攻击。

3、信息技术和运行技术的有关法规要求和标准

工业物联网系统的实施和运行必须遵守相关法规和合规性要求。来自运行技术背景的人员应拓宽视角，考虑各种互联系统的安全性。具有信息技术背景的人员必须考虑安全规定以及工业物联网系统与安全规章的关系。新的立法也有望对信息技术和运行技术提出更多的审计、保证及合规性要求，以涵盖整个工业物联网系统。

4、运行技术的棕色地带

棕色地带是指一种环境，在该环境中，传统解决方案与新解决方案和组件相互交织，共同存在。运行技术系统通常位于棕色地带。按照信息技术的安全标准，大多数工业设备均已“老化”或“过时”。由于目前许多系统仍然依赖于物理安全（门锁和守卫）、运行技术网络的隔离和工业协议的模糊性以弥补网络安全的缺失，但这并不凑效。在攻击者看来，旧式运行技术系统是理想的攻击目标，安全保护措施过时导致许多工业系统易遭受破坏。

对目前运行在棕色地带的运行技术环境实施安全措施时，应

尽量选用非侵入方式，采取如防火墙、路由器等网络边界保护防护措施，以强化运行技术控制环境及网络外部与控制系统的隔离效果。

5、工业物联网的云系统

工业物联网的优势之一，是能用外部网络计算能力对运行技术基础设施进行分析和控制。在典型的工业物联网系统中，数以千计的设备与云系统进行通信，甚至在云系统存储数据。利用第三方提供的共享服务，会形成数个信任边界，从而影响安全性和隐私性。流向控制系统的信息流必须妥善加以保护，以确保物理流程的安全性和弹性。

（四）保障工业物联网安全的意义

未来若干年，运行技术系统和信息技术系统会在不断变化的终端、通信、监控和管理系统环境下实现整合，从而达到所需的安全要求。基于安全考虑，有必要对业务和实施过程加以改进，对与人或环境安全相关的设备进行认证，对新的攻击与威胁模式加以评估，以确保工业物联网系统安全。

二、工业物联网组织、架构与技术层面的安全评估

（一）风险管理

消除系统的所有风险并不现实，人们必须进行风险管控，在

安全费用与安全成效之间找到最佳平衡点。为管控风险，必须对各安保措施进行评估，决定投资何种安保计划，并定期对风险与计划成效进行重新评估。应对安全风险的措施包括**规避风险、缓解风险、转移风险、接受风险、剩余风险以及有效的经营决策等。**

风险并不是静态的。系统概念、价值或关键性发生变化；系统的物理构成发生变化；系统面临的威胁发生变化；现有能力发生变化或增加新的特征等都可能导致风险发生变化，因此需定期对风险进行评估。

（二）风险评估

风险评估是一个对风险、尤其是信息安全风险进行表征的过程。工业物联网的风险评估既包含对发生错误或遭受攻击时产生的物理后果的评估，也包含对信息系统风险的典型评估。尽管预测各种潜在威胁并不现实，但一个能应对多种运行环境变化的强大的安全模型能有效缓解许多无法预测情况对系统造成的影响。

（三）风险交流

有效经营决策是工业安全保障的重要组成部分，制定决策时，不同安全风险和防御姿态的成本与效益信息应清晰传达给决策人员，尤其是在其不熟悉安保风险和应对措施细节的情况下。风险交流的基本方式包括**定量风险评估、定性风险评估和系统方法**三种。对高发性、低影响力事件的风险一般采用定量风险评估，

对低发性、高影响力事件以及经营决策人员难以进行评估的风险，一般采用定性风险评估。

（四）关键风险性能评价指标

从构想到设计制造，再到最后的投入运行，经营决策人员应全程对工业物联网系统的安全情况进行监测，且监测力度应与性能、生产量、成本、效率等其他特性监测相同。制定相应评价指标和基线时，应充分考虑主要相关方在系统行业部门的利益需求、法律责任和行为规范。此外，还应对上述所有考虑因素定期进行审查，以便做出适当调整。

三、工业物联网的安全运行

工业物联网系统的运行必须提供从边缘到云端的端到端安全保障机制，包括加固端点设备、保护通信、管控策略与设备更新，以及利用分析工具和远程访问实时管理与监测整个安全保障流程。安全保障机制必须融入设计，且尽早对风险进行评估。制造商、系统集成商、设备所有者以及运营商都必须参与其中，以创建一个更加安全可靠的工业物联网系统。

鉴于工业系统具有独立性的本质特征，安全保障措施的实施应适用于多种环境。安全保障计划的实施应全面考虑对系统的功能性和非功能性需求，包括相对优先顺序。安全保障措施的实施

也需要人参与，通过监测状态与审查分析工具，来进行必要决策，并实施修正与改进规划。有效的管控系统可以降低人为操作失误，提升系统安保性能。

（一）安全框架

工业互联网安全框架由六个相互作用的模块构成，如图 2 所示。这六大模块可分为三层，顶层包括四种关键安全保障功能：端点保护、通信与连通性保护、安全监测与分析、安全配置与管理，这四种功能均以数据保护层和全系统安全模型与策略层为支撑。

图 2　安全架构功能图

端点保护在边界和云端执行防御功能，主要关注点包括物理安全功能、网络安全技术和管理员身份。**通信与连通性保护**通过来自端点保护的管理员身份功能来执行流量验证与授权，运用加密技术以及信息流控制技术可以为通信和连通性提供保护。在实现端点和通信安全的基础上，对系统所有组件进行**安全监测与分析**以及**安全配置管理**，能确保系统在整个运行生命周期的安全。**数据保护层**既能保护静态端点数据，也能保护动态通信数据。**安全模型与策略**管控着安全措施的实施以及系统在整个生命周期的保密性、完整性和可靠性。

（二）六大模块

1、端点保护

端点是指工业物联网系统中既包括计算和通信功能，还包括其他功能性接口的外接件，可能是边缘设备、通信基础设施、云服务器，也可能是任意中间设备。每个端点的要求和硬件制约条件各不相同，并且影响着可以达到的安全等级。因此，应根据具体的功能和安全要求采用相应的安全保障机制与技术。端点保护功能如图 3 所示。

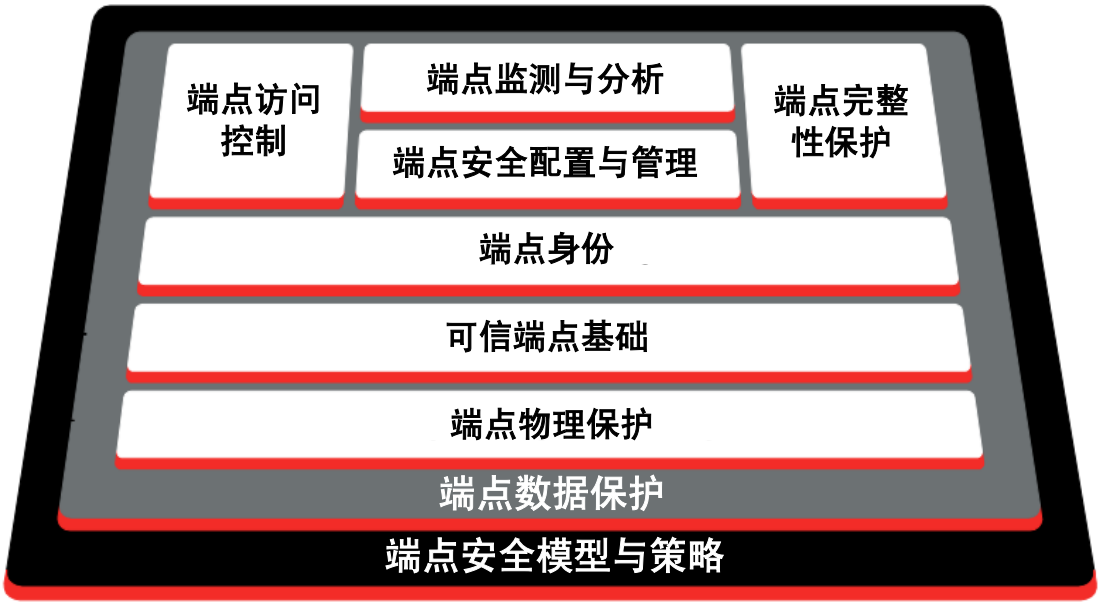

图 3　端点保护功能示意图

端点保护旨在确保端点功能的可用性、保密性和完整性。端点安全功能包括**端点物理保护、可信端点基础、端点身份、端点完整性保护、端点访问控制、端点安全配置与管理、端点监测与分析、端点数据保护、端点安全模型与策略**等。

2、通信和连通性保护

通信和连通性保护旨在为端点到网络的连通性提供物理保障，保护网络中的信息流和端点之间的通信加密。为保护和控制动态数据，通信和连通性安全重点考虑**连通性的物理安全、通信端点保护、加密保护、信息流保护、网络配置与管理、网络监测与分析、动态数据保护、通信与连通性保护策略**等功能。

3、安全监测与分析

安全监测与分析用于从端点和连通流量中抓取系统整体状

态的数据，然后加以分析，以探测可能的安全违章或潜在的系统威胁。一旦探测到上述问题，根据系统安全策略，采取各种应对措施。这种监测-分析-行动的循环可以实时完成，也可以稍后完成，从而明确应用模式并探测潜在的攻击场景。

安全监测与分析包括**监测、分析和行动**3项最重要的功能。其中监测功能的数据来源于**端点与通信、安全远程日志以及供应链**；分析类型包括**行为分析**和**基于规则的分析**；行动类型分为**主动型/预测型行动、反应型探测与恢复行动以及根源分析与取证行动**。

4、安全配置与管理

安全配置与管理用于控制系统运行功能（包括可靠性和安全行为）和安全控制的变更。安全配置管理包括**安全运行管理、安全管理、端点身份管理、端点配置与管理、通信配置与管理、安保模型变更控制、配置与管理数据保护、变更管理的安保模型与政策**等功能。

5、数据保护

数据遍布整个工业物联网系统。每组数据具有不同的生命周期、关联时间和与泄露相关的潜在风险，数据的修改、拦截或复制都有可能带来上述威胁。攻击会对数据造成各种不同影响，包括系统性能的变化或对未来系统造成不利影响。需要保护的数据

类型包括**端点数据、通信数据、配置数据**和**监测数据**。

6、安全模型与策略

安全模型与策略涵盖规章制度、组织架构和机器安全等级三个方面。安全策略是指系统的安全目标，安全模型则是系统安全策略的正式表达形式。安全模型与策略的主要功能包括**系统威胁分析、系统安全目标、安全策略、安全模型、数据保护安全策略、端点安全策略、通信与连通性安全策略、监测与分析安全策略、配置与管理安全策略**等。

（三）端点保护详述

1、安全威胁与端点的可能漏洞

端点存在许多潜在漏洞，容易被有意或无意的错误利用。每种配置也都有其优劣势，针对各种应用必须加以评估。端点存在威胁和漏洞的领域包括**变更硬件组件与配置、操控或劫持系统开机程序、损坏操作系统、虚拟化管理系统和分立内核、非法变更应用软件或应用编程外部接口、部署程序漏洞、恶意更改端点数据、破坏监测与分析系统、配置与管理漏洞、非法变更安全策略与模型、开发环境存在漏洞**等。为保障端点软件的完整性，需要从整个开发和运行生命周期内搜集证据，以避免、消除或修复潜在威胁，并标记该基线，用以验证启动时加载正确的软件。

2、端点的物理安全

端点部署在各种环境中，对于保护资产免受盗窃、篡改、破坏有不同的安全要求。工业系统中广泛采用物理访问技术防止非法用户物理接触端点和通信设备。有些端点，如智能仪表和环境传感器，必须安置在安全物理边界之外。

物理围栏有助于提供破坏者证据，防止非法随意篡改。物理外壳可提供稳定的运行条件。应对端点物理访问外围设备端口（如 USB）进行控制，防止非法外围设备接入端点。根据威胁模型，端点应采用防篡改软件组件或其他安全存储设备，以防关键数据被盗。

3、端点身份验证和接入控制

端点身份模块在正确的身份验证基础上，可实现各种安全控制。身份是一个实物区别于其他实物的固有属性，证书是支持身份声明的证据，证书的常见类型为加密证书（如 X509 数字证书）。端点的可信度可分为若干等级，具体取决于特定物联网工业系统的威胁模型。每种信任等级都决定了证书的最低安全保障能力，包括证书的唯一性、证书存储和证书使用（如认证、授权等）。

端点访问控制依赖于认证和授权，认证能确保实物特征的正确性；授权是指授予权限，包括根据访问权利授予访问权限。授权取决于对实物身份映射的验证，授权依赖于认证。人类和非人

类实体必须拥有证明自己身份的证书，用于认证、识别和授权。

4、端点数据保护

端点数据保护包括静态数据保护和应用数据保护。边界、云端和通信动态数据的保护策略各不相同。加密可保护数据的保密性和完整性，适用于所有数据的保护，而保护部分敏感数据，需要保护整个存储介质。在实践中，可能会同时采用多种数据保护技术，以防止不同类型的攻击。

5、端点监测与分析

监测机制也应加以保护。端点监测主要用于探测可能的设备变更和损害，以防错误事件报告。端点安全状态的监测可能在端点内部进行，也可能在端点外部进行，而对最低能力的边缘设备的监测则很可能从操作域的另一个端点进行。

6、端点配置与管理

端点须为其组件提供安全、可控的更改（尽管极少数情况下并不要求安全性能）。应对所有更新和更改进行签名，对其有效内容进行加密，并记录操作，以便后续审核和恢复端点，而这些服务应该以非侵入方式提供给操作功能。

7、端点保护的加密技术

加密技术给出了数据转换的原则、手段和机制，以隐藏信息内容，防止数据被非法修改或使用。在端点处，通过加密技术可

执行大量安全操作。端点必须采用标准加密算法，秘钥必须是随机且无法预测的，还要有足够的字长，以排除对可用秘钥空间的暴力破解或遍历搜索。

8、端点保护的隔离技术

隔离技术用于保护系统组件不受有害影响，如保护端点元件不受其他端点元件的影响，以免其功能发生故障或遭到破坏。常见隔离模型包括**程序隔离、边界隔离、虚拟隔离和物理隔离**。

译自：*Industrial Internet of Things, Volume G4: Security Framework by Industrial Internet Consortium*

赛迪智库
面向政府 服务决策

咨询翘楚在这里汇聚

信息化研究中心	工业化研究中心	规划研究所
电子信息产业研究所	工业经济研究所	产业政策研究所
软件产业研究所	工业科技研究所	军民结合研究所
网络空间研究所	装备工业研究所	中小企业研究所
无线电管理研究所	消费品工业研究所	政策法规研究所
互联网研究所	原材料工业研究所	世界工业研究所
集成电路研究所	工业节能与环保研究所	安全产业研究所

编 辑 部：赛迪工业和信息化研究院
通讯地址：北京市海淀区万寿路27号院8号楼12层
邮政编码：100846
联 系 人：刘 颖 董 凯
联系电话：010-68200552 13701304215
010-68207922 18701325686
传 真：0086-10-68209616
网 址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门，
相关部门及研究单位，相关行业协会

编 辑 部：工业和信息化部赛迪研究院

通讯地址：北京市海淀区紫竹院路 66 号赛迪大厦 15 层国际合作处

邮政编码：100048

联 系 人：韩宇雪

联系电话：（010）88559543　18610215602

传　　真：（010）88558833

网　　址：www.ccidgroup.com

电子邮件：hanyx@ccidgroup.com