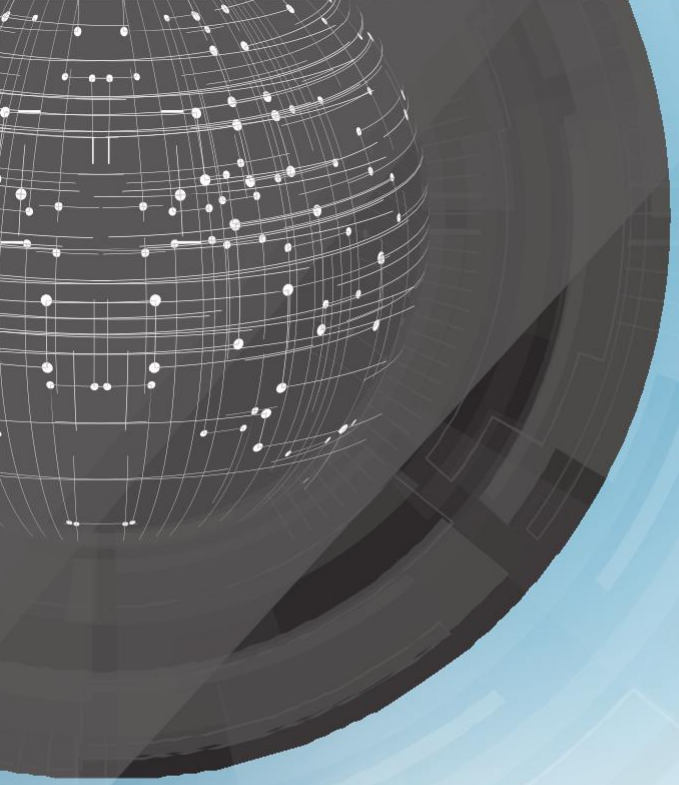


物联网安全控制框架指南

致谢

发起人：

Brian Russell

Michael Roza

关键贡献者：

Hillary Baron

Luciano Ferrari

Aaron Guzman

Ankur Gargi

Sabri Khemissa

Douglas Mcdorman

Todd Nelson

Eric Palmer

J.R. Santos

Theodoros Stergiou

Srinivas Tatipamula

John Yeoh

CSA 大中华区专家翻译：

余晓光 、何国锋、刘德林、薛永刚、郭鹏程、吕浩、刘宇馨、乔思远、姚凯、刘洪森、石新美、张振国

C-CSA 工作人员：

史晓婧、胡锦涵

关于CSA 物联网工作组：

设备互联和赛博物理系统在企业环境中变得越来越普遍。随着云端环境的扩展到包含这些技术，万物互联的世界依赖于通过设备来管理、编排和同步数据。CSA物联网工作组开发框架、流程和最知名的方法来保护这些连接的系统。物联网工作组致力于研究的专题包括数据隐私、雾计算、智慧城市等。从这里了解更多。

序言

云安全联盟CSA已经成立了十年，过去的十年是云计算从萌芽到茁壮成长的时代，CSA通过云安全指南和云控制矩阵等重要安全白皮书引领业界在技术，标准，认证等方面发展。未来的十年，物联网设备将使连接各种云平台的终端增长数十倍达到上千亿台，可以说下个十年是物联网时代，安全将受到更大的挑战，物联网安全威胁从数字世界延伸到物理世界，危及人身安全。在这项新兴技术和新兴威胁来临之际，CSA IoT工作组通过前瞻性的研究取得了多项成果，发布过《物联网安全指南》，《用区块链技术保障物联网》等内容，这次CSA物联网工作组发布《物联网控制框架》及《物联网安全控制框架指南》，它在物联网时代的重要意义相当于云计算时代的云控制矩阵，将成为业界的物联网系统设计、部署、检测基石，有望再次被誉为CSA贡献的安全黄金标准。

在此，感谢CSA大中华区研究院与C-CSA专家委员会的专家们及时地把白皮书翻译成中文，供大家学习。

李雨航 Yale Li

云安全联盟大中华区主席

中国云安全与新兴技术安全创新联盟执行理事

术语

原文	翻译
access	访问
Administrator	管理员
assessment	评估
audit	审计
audit log	审计日志
Authenticate	认证
authorize	授权
authorized roles	授权角色
availability	可用性
baselines	基线
Certificate	证书
certificate revocation	证书撤销
cloud	云
Component	组件
compromised	受损的
confidentiality	保密性
configuration	配置
credential	身份凭据
data classification	数据分类
data type	数据类型
data value	数据价值
edge device	边缘设备
encrytion	加密
firmware	固件
firmware image	固件镜像
fog	雾
forward-secrecy	前向安全性
Framework	框架
gateway	网关
governance	治理
Identify	识别
integrity	一致性/完整性
IoT device	物联网设备
IoT system	物联网系统
key derivation	密钥派生
key lifetime	密钥周期
key management	密钥管理
key update	密钥升级
Keys	密钥
level of control	控制水平
malicious code	恶意代码
organization	组织

minimum access security 最低安全要求

password 密码

patch 补丁

policies 策略

privilege 特权

Procedure 过程/程序/步骤

process 处理

remote access 远程访问

risk 风险

risk impact 风险影响

RTOS 实时操作系统

security log 安全日志

sensitivity 敏感性

service 服务

signature 签名

tamper 篡改

third party 第三方

third party component 第三方组件

third party library 第三方库

trusted mode 可信模式

unauthorized actors/users 非法用户

validate 验证

zeroizate 归零化

Opertional Certificates 操作

目录

简介

《云安全联盟(CSA)物联网(IoT)安全控制指南》提供了CSA物联网安全控制框架的使用指导。本指南用于指导您如何使用框架对您的组织进行IoT系统的评估和实施。欧洲网络与信息安全署（ENISA）[1]将物联网系统定义为“互联传感器和执行器的赛博物理生态系统，可实现智能决策。”

物联网安全控制框架与企业物联网系统相关，包括多种接入设备、云服务和网络技术。无论是处理只有有限影响潜力的“低价值”数据还是支持关键业务的高度敏感系统。该框架在许多物联网领域有实用价值，从系系统的划分是由系统所有者根据存储和处理的数据的价值以及各种物理安全威胁的潜在影响而分配的。

该框架帮助用户识别合适的安全控制，并将其分配给其物联网系统中的特定组件，包括但不限于以下组件：

- **简单传感器**
- **简易执行器**
- **边缘设备**
- **雾计算**
- **移动设备/应用**
- **前置中间设备**
- **云网关**
- **云应用/服务**

目标读者

设计和开发人员经常被要求创建安全的物联网系统，或者对其它物联网系统进行评估。物联网安全控制框架是为这些设计人员和开发人员所提供的资源。设计人员和开发人员可以使用这个工具，在整个物联网系统实施开发的周期中不断评估实现的安全性。通过对物联网系统的整体评估，确保物联网系统满足业界最佳实践。

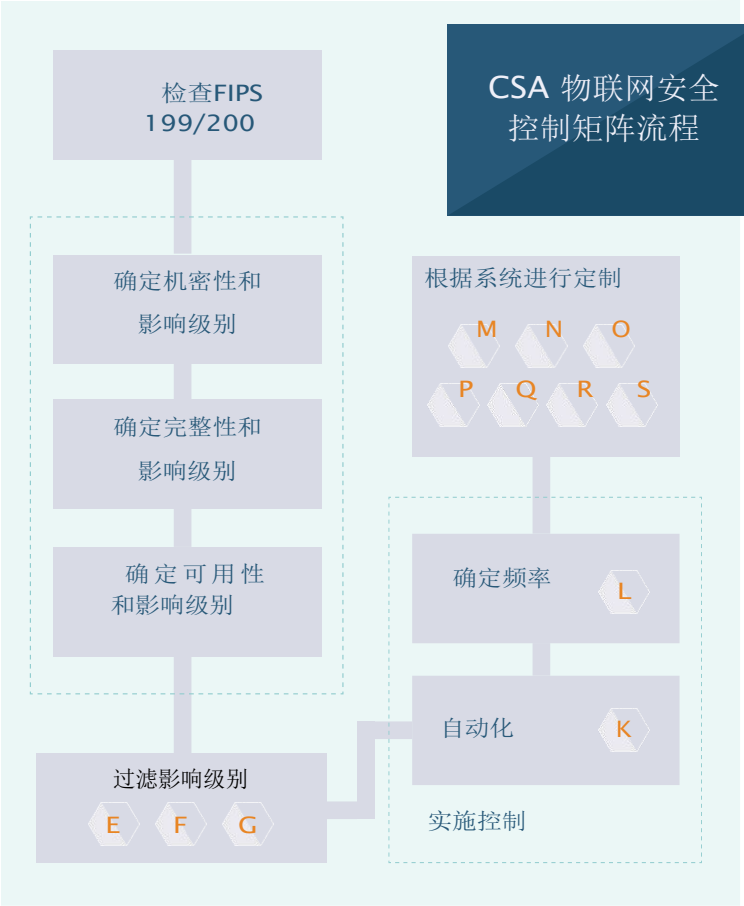
版本

物联网安全控制框架的第一版引入了基础级别的安全控制，以减轻在一系列威胁环境中运行的物联网系统所带来的诸多风险。CSA对本框架后续版本的计划包括开发适用的测试指导以及其他领先的物联网安全组织同步业界最佳实践。

[1] https://www.enisa.europa.eu/news/enisa-news/defining-and-securing-the-internet-of-things/

如何使用CSA物联网安全控制框架

图一详细说明了CSA物联网安全控制框架的用户在评估并实施其特定环境的安全控制时应遵循的流程。此插图中的圆圈字母与框架(电子表格)中的列相对应。



安全控制的目标
(A, B, C, D列)

控制域	控制 ID	云控制矩阵标识

控制域 (A列): 对D列（控制规范）中详细描述的个人安全控制根据逻辑进行分组，每一个相应的控制规范的名称在控制领域的类别下面用斜体字标示。

控制ID (B列): 特定安全控制的官方标识、关联的字母和编号（例如“RSM-01”）允许控制项在其他地方通过控制项在框架中的位置进行引用。

CCM ID (C列): 框架中的安全控制在此列中被关联或映射到CSA 云控制矩阵 (CCM)中的标识符。当IoT安全控制被派生或链接到一个CCM控制时，就会识别一个或多个条目。关联控制涉及到对每个框架中控制规范的部分覆盖或完全覆盖。

控制规格范(D列)： 规范作为应对物联网特定风险区域的消除措施或应对措施。从可用性出发，为了应对特有的物联网环境，每个控制措施被分解成一个简化的动作。

物联网系统风险影响级别

（E，F，G列）

物联网系统风险影响水平		
机密性	完整性	可用性

E到G列 ： 允许用户根据特定环境制定安全控制措施。用户制定安全控制措施时，应参照美国商务部的两个标准：“联邦信息和信息系统安全分类标准”（FIPS 199）和“联邦信息和信息系统的最低安全要求”（FIPS 200）这两个标准[2]。FIPS 199和200将风险影响级别分为低、中或高三个等级：

机密性（E列）： 物联网系统中的某些数据，如个人隐私信息和专有信息，需要通过各种安全控制进行访问控制，保证适当的机密性。评估物联网系统组成部分的机密性风险，需要评估该系统数据被公开或被攻击者破坏时可能会产生的影响（低、中或高）。

完整性（F列）： 为保护数据完整性，企业必须防止对数据进行不正确的修改或破坏，并确保信息真实性。评估物联网系统不同组成部分的完整性风险，需要评估流经系统的数据被破坏或不当修改后的影响（低、中或高）。

可用性（G列）： 评估系统中需实时可靠访问信息的可用性程度，需要评估系统如果无法运行时的的潜在风险。

评估有关系统数据的机密性，完整性和可用性采用低中高三个等级，请参阅FIPS 199第6页的表1：“对安全目标的潜在影响的定义”。

确定这些风险影响级别后，可以使用IoT安全控制框架来确定需要在环境中实施的所需安全控制措施。

---

[2]FIPS 199：“联邦信息和信息系统安全分类标准”，联邦信息处理标准出版物，计算机安全部，美国商务部；2004年2月.https：// nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FIPS 200：“联邦信息和信息系统的最低安全要求”，联邦信息处理标准出版物，计算机安全部，美国商务部；2006年3月.https：// nvl-pubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

注意，当影响级别为高时，必须应用所有的安全控制，包括针对低、中和高风险级别的安全控制措施在内的所有安全控制措施。 当影响级别为中等时，需要采用所有针对中和低风险级别的安全控制措施。

以下是三个影响级别和对应安全控制措施的示例。

安全风险类型	风险影响级别	必要安全控制
机密性	高	高、中、低
完整性	中	中、低
可用性	低	低

补充控制措施指导

（H列，I列）

补充控制指南	
附件说明	引用 / 解释

附加说明（H列）：在物联网安全控制框架中评估或实施任何单个安全协议时，请务必查看该项详细说明特殊要求的补充信息，术语解释，相关操作提示等的补充信息。

参考文献/解释（I列）：本列提供包括官方出版物，法规信息以及便于完全理解控制规范所需的其他参考资料的相关专业来源的信息。

实施指南

（J，K，L列）

实施指南		
安全控制类型	*控制实施*	*控制频率*

如果为企业实施安全计划，请使用“实施指南框架”中的部分来帮助确定企业特有环境所需的控制类型（J列）；该组织将如何实施控制措施（K列）；以及每种安全控制措施的必要频度（L列）。

安全控制措施的类型（J列）

物联网框架中的安全控制措施根据何时、何地以及措施如何提高安全性分为三种类型。

预防性措施：可以阻止某些安全事件的发生，例如通过锁门或使用更高级别的生物识别限制物理访问房间。

侦测性控制措施：识别并提取事件特征。 如通过盘点发现库存差异；录制视频；并使用运动传感器检测非法侵入。

纠正性控制措施：减轻安全事件造成的损害，例如灭火器可以减少火灾的潜在影响，或者在主数据中心发生故障时可以使用备份的数据中心。

控制措施的实施（K列）

安全控制措施根据自动化级别有三种实现方式。

手动控制由人员执行。 例如，在风险管理流程审核中，通过人员评估来确认流程是否已依据策略执行。

自动控制由系统执行，无需人为干预。 例如，在用户访问检查中，用户使用用户名和密码登录，系统在验证其组合正确后授予访问权限。

半自动控制结合了自动和手动操作。 例如，在实际仓储中，物品被清点并将结果与系统生成的列表进行比较， 通过调查调整差异使库存和系统记录一致-，这就会涉及纸质和电子记录。

控制措施的实现频率（L列）

根据各个企业的不同需求，执行安全控制措施时需要不同的频率。 一些组织需要根据内部风险优先级或合规要求进行更频繁的控制。 建议在不同情况下使用以下频率：

- 每年
- 每季度
- 每月
- 每周
- 每天
- 事件：控制不规则地执行，例如在软件更新时
- 连续：每天多次控制，例如用户访问权限

物联网系统中的边缘组件，雾计算组件和云组件

（ M列到S列）

物联网系统组件-边缘，雾和云						
边缘			网络			云
简单传感器	简单执行器	复杂边缘设备	雾/网络计算层	移动应用	本地网关	云服提供商

通过M到S列确定要求是否适用于物联网系统组件。例如，某些要求可能仅适用于边缘设备，而其他要求可能仅适用于网关或云服务。 物联网安全控制框架旨在根据特定物联网系统实施定制化的安全要求。 在这方面，边缘，网络和云等物联网系统中的常见组件，已经确定了相应要求。

边缘（M，N，O列）

在物联网边缘，数据通过各种传感器从物理世界输入，并且通过各种形式的输出设备和执行器采取动作改变物理状态。边缘设备执行分析并生成知识，最大限度地减少中央数据中心和连接系统之间进行通信的带宽要求。 例如，自动驾驶汽车可以连接到云或数据中心，但也需要在位于边缘节点的站点进行分析和处理以确保安全。 在边缘运行分析还可以包括靠近的设备间的协作或与有用的相关技术的协作。边缘计算[3] 还可以促成智能和协作制造过程。例如，可以向下游设备通知上游过程中的延迟，然后可以在解决问题时采取措施保存能量。

简单传感器（M列）： 边缘设备在处理、存储和网络方面的能力非常有限。 这些设备的特征示例包括电池电量；节省电力的睡眠模式；用于捕获和传输单个信息如压力或温度的微控制器等。 应用于这些传感器的安全控制仅限于他们的硬件功能。 但是，可以在网关或云等其他级别（例如网关或云中）向这些传感器添加安全性。

简单执行器（N列）： 这些边缘设备在处理，存储和网络能力方面也受到限制，但执行操作泵一类的物理功能，与简单的传感器一样，它们通常不具备配备强大的安全控制措施。

---

[3] https://en.wikipedia.org/wiki/Edge_computing

复杂边缘设备（O列）：能够满足高级别安全要求的设备，例如一体化软件或硬件加密安全模块。

网络（P，Q，R列）

在网络中，雾计算节点（P列）执行分析，节点管理和策略管理。基础设施设备，如本地物联网网关（Q列），汇集来自各种物联网设备（如无线传感器网络）的数据。移动应用程序（R列）与物联网设备和相关的云服务对接，支持远程管理等一系列物联网服务，包括远程管理。

雾/网络计算层（P列）：由美国商务部（NIST）国家标准与技术研究所定义如下：

> “雾计算4是一种分层模型，能够无处不在地访问可扩展计算资源的共享连续体。 该模型有助于部署分布式，对延迟敏感的应用程序和服务，并由驻留在智能终端设备和集中式（云）服务之间的（物理或虚拟）雾节点组成。 雾节点是上下文感知的并且支持公共数据管理和通信系统。它们可以按集群组织 - 可以是垂直的以支持隔离，也可以是水平的以支持联合，或相对于雾节点到智能终端设备的延迟距离。 雾计算最大限度地减少了支持应用程序的请求 - 响应时间，为终端设备提供本地计算资源，并在需要时为集中服务提供网络连接。

在雾层，节点从物联网设备实时接收反馈。 雾节点运行支持IoT应用程序进行实时控制和分析，响应时间为毫秒。 节点提供瞬态存储，通常为1到2小时，然后将定期数据摘要发送到云[5]。

移动应用程序（Q列）：与IoT设备或服务配对或交互的应用程序或用户界面。

本地网关（R列）：网关是边缘设备的连接或控制器，例如本地应用层的MQTT代理和聚合本地无线传感器网络（WSN）通信的通信网关。

云（S列）

云服务提供商或CSPs（S列）：连接到边缘设备的云应用程序，服务和网关支持一系列物联网功能，包括机器学习，语音识别，事件处理，数据分析，消息传递，通知，数据库管理和注册和日志记录等网络安全服务。 云中的网关连接到边缘设备。 这些网关是应用层网关（例如MQTT代理）或CSP前面的通信网关。

---

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf
[5] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

其他资源

富士通开发的数据处理架构“Dracena”可以重新配置物联网数据处理流中的内容；富士通实验室有限公司，日本川崎，2018年3月7日。

http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0307-02.html

《物联网国际网络安全标准化现状跨部门报告》(美国国家标准化与技术研究所联合报告8200 草案)；美国国家标准与技术研究院;2018年2月。
https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200- draft.pdf

“关键信息基础设施背景下的物联网基线安全建议”，欧盟网络和信息安全局（ENISA）; 2017年11月20日。
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

“物联网 - 参考架构”，ISO / IEC JTC 1 / SC 41；2018年8月。
https://www.iso.org/standard/65695.html

《医疗设备网络安全的上市后管理:对行业和食品药品监督管理局工作人员的指导》，美国食品药品监督管理局(FDA)，第4节;2016年1月22日。
https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

“可互操作医疗器械的设计考虑和上市前提交建议：工业和食品药品管理局工作人员指南”，美国食品药品监督管理局(FDA); 2016年1月26日。
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf

“美国食品药品监督管理局(FDA)情况说明书”，“FDA在医疗设备网络安全中的作用:消除神话、了解事实”。
https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf

“可信和安全的无线传感器网络设计和部署”，作者：Ignacio Bravo，Esther Palomar，Alfredo Gardel和JoséLuisLázaro; 传感器：一个开源期刊，2017年8月4日。
http://www.mdpi.com/1424-8220/17/8/1787/pdf

“传输层安全（TLS）实现的选择、配置和使用指南”，美国国家标准与技术研究院NIST SP特刊（SP）800-52修订版1；2014年4月。
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

“安全使用传输层安全性（TLS）和数据报传输层安全性（DTLS）的建议”，“互联网工程任务组（IETF）RFC 7525；2015年5月。
https://tools.ietf.org/html/rfc7525

“Internet of Things Security Best Practices,” Microsoft Azure.
“物联网安全最佳实践”，微软Azure。
https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices

由Jeffrey Voas、Richard Kuhn、Phillip Laplante和Sophia Applebaum合著的《物联网信任问题》;NISTIR 8222;2018年9月。
https://csrc.nist.gov/publications/detail/nistir/8222/draft

由Elaine Barker和Allen Roginsky合著的《过渡:关于密码算法和密钥长度使用的过渡建议》(transition: Recommendation for transition for the Use of Cryptographic Algorithms and Key length);NIST SP 800-131A修订版1;2015年11月。
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

由Kaitlin Boeckl、Michael Fagan、William Fisher、Naomi Lefkovitz、Katerina Megas、Ellen Nadeau、Ben Piccarreta、Danna Gabel O 'Rourke和Karen Scarfone合著的《管理物联网(IoT)网络安全和隐私风险的考虑因素》；美国国家标准化与技术研究所联合报告 8228(草案)，2018年9月。
https://csrc.nist.gov/publications/detail/nistir/8228/draft

由Michaela Iorga, Larry Feldman, Robert Barton, Michael J. Martin, Nedim Goren和Charif Mahmoudi撰写的《雾计算概念模型，美国国家标准与技术研究所的建议》;NIST SP 500-325, 2018年3月14日。
https://www.nist.gov/publications/fog-computing-conceptual-model

《雾计算概念模型:国家标准与技术研究所的建议》，美国国家标准与技术研究所NISTSP 500-325。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf