ICS 35. 040
L 80
备案号

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0006-2024

信息安全技术
工业物联网安全等级评价模型

Information security technology

Industrial Internet of Things security grade evaluation model

天津市商用密码行业协会 发布

目录

前　言

本文件根据 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由天津市商用密码行业协会归口。

本文件起草单位：天津大学、天津光电安辰信息技术股份有限公司、天津光电通信技术有限公司、天津光电通电子科技有限公司、天津云安科技发展有限公司、宝牧科技（天津）有限公司、河北承高智慧交通有限公司、聚能信安（天津）科技有限公司、轩辕（天津）智能科技有限公司。

本文件主要起草人：胡双喜、许光全、钟明旸、申烨、焦庆玲、曹晓冬、贾玉凤、姚嘉、张文涛、李智超、李若甫、宋津津、毕建宇、吴俊、吴超、徐文大、郑晨、李长宇、张璐琳、徐洋。

引　言

随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统，包括分布式控制系统、监控与数据采集系统和可编程逻辑控制器等产品广泛应用于冶金、电力、石化、水处理、铁路、航空和食品加工等行业。工业控制系统由单机走向互联、从封闭走向开放、从自动化走向智能化进程的加快，使得工业控制系统成为工业生产中至关重要的部分，而与此同时，工业控制系统的信息安全问题日益突出，工业控制系统的安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。对此，全国信息安全标准化技术委员会立项研制了工业控制系统信息安全分级、管理要求、控制应用指南等多项标准。

本标准制定的目的是为使用工业物联网系统的行业进行信息安全建设以及国家政府机构对国家重点行业进行信息安全检查中选择和指定的安全控制提供评价模型。本标准制定的目标是指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评估工作，及时有效发现工业物联网系统存在的突出问题，为国家对重点行业工业控制信息安全检查时根据评估模型得到量化得分，及时发现工业物联网的信息安全缺陷。

信息安全技术 工业物联网评价模型

1 范围

本标准规定了工业物联网安全评价模型，包括工业物联网管理、技术设计、工程实现多个维度，并针对工业物联网信息系统的评价过程给出完整的量化模型。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 7665-2005 传感器通用术语

GB/T 20984-2022《信息安全技术信息安全风险评估方法》

ISO/IEC62264-1-2013 《企业控制系统综合--第 1 部分：模型和术语》

GB/T 22239-2019 《网络安全等级保护基本要求》

GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》

3 术语和定义

GB/T 25069-2010 中界定的及下列术语和定义适用于本文件。

3.1 传感器 transducer/sensor

能感受被测量并按照一定的规律转换成可用输出信号的器件或装置，通常由敏感元件和转换元件组成。

注：GB/T 7665-2005 定义了传感器的一般分类术语，其中从被测量角度定义了三类传感器，即物理量传感器、化学量传感器和生物量传感器。

3.2 感知终端 perception terminal

物联网信息系统中能对物进行信息采集和/或执行操作，并能联网进行通信的装置。感知终端根据是否具有操作系统,可分为具有操作系统的感知终端和不具有操作系统的感知终端。

3.3 质量保证工程师 Quality Assurance / QA

一种工程进行中的岗位，主要职责是对软件产品及其相关文档进行测试，确保软件产品的质量符合规范和用户需求。

3.4 分布式控制系统 DCS distributed control system

以计算机为基础，在系统内部（单位内部）对生产过程进行分布控制、集中管理的系统。在本文特指工业物联网中，用于控制、管理、交互工业生产中的各种设备的系统。

4 工业物联网评价模型

4.1 模型概述

并非所有工业物联网系统都需要相同强度的保护机制来满足其安全要求。系统管理员需首先确定促进安全增强过程的优先级，使保护机制在不超出必要范围的情况下适应其组织安全的目标。如果预期安全机制和流程的实施能够有效地实现这些目标，则认为这些措施是成熟的。决定成熟度的是安全机制在解决目标方面的适当性，而不是它们的客观强度。因此，安全成熟度是当前安全状态满足所有系统安全需求和要求的置信度。也就是说，安全成熟度是衡量对包括人员、流程和技术在内的整体安全级别的理解程度，包括其支持的必要性、收益和成本，促成因素包括对组织系统的垂直行业、安全、监管、道德和合规要求的特定威胁，以及系统威胁概况和环境中存在的独特风险。

4.2 模型要求与范围

现实世界的适用性：设定安全成熟度目标的方法必须考虑功能、安全、监管和法律要求或准则、风险管理、安全和隐私政策、性能、成本和其他业务考虑。此外，还必须考虑已知的和新出现的威胁，以及应对这些威胁的可负担的方法。该过程的结果和实现目标的指导应直接适用于有关的物联网基础设施，这要求该过程是可操作的。

对不同角度的考虑： 安全评估模型有助于从不同的角度描述安全成熟度，包括业务和实施角度。它有助于从组织角度定义安全成熟度目标，从实施角度定义安全成熟度要求。该模型有助于调整这些定义，从而推动所有致力于提高安全成熟度的相关人员之间的合作。

适当的安全指导： 安全评估模型为评估和进一步提高安全成熟度提供指导，使安全能力与特定用例相一致。指导应该是实用和可操作的。

可适应不断变化的威胁环境： 随着基础设施和威胁的发展，安全目标必须具有适应性（如固件更新或补丁），以保持长期的相关性。对于运行寿命长的系统，仅在系统设计阶段实施安全措施是不够的。

可扩展性： 物联网商业模式、产品、准则、法规、技术和组织类型将不断发展。安全评估模型需要有足够的灵活性来适应任何变化。

安全评估模型解释了如何以有效的方式将安全实践与现有的安全问题结合起来。安全评估模型提供了安全实践的分类和详细描述，其安全成熟度的标准，相关的安全问题，技术和能力，允许根据既定的战略评估和规划其实施。此外，安全评估模型还提供了关于这种评估和实施过程的建议。

4.3 模型域

4.3.1 域、子域与实践

管理、实现和加固等领域决定了战略层面上安全成熟度提升的优先级。管理是由一个组织的管理员制定策略，并持续监督其正确实施；实现是指实施安全控制和实践，以创建一个满足策略和操作要求的系统；加固是在系统运行期间使用安全实践。

在规划时，可根据风险分析和其他因素，将不同的优先级放在不同域和子域上，随后的实现将根据这些优先级来使用这些实践。域和子域还有助于从逻辑上组织实践，清楚地

说明在哪些地方可以使用不同的替代方案来满足特定域或子域的要求。图 4- 1 显示了模型域及相关子领域及实践的层次结构。

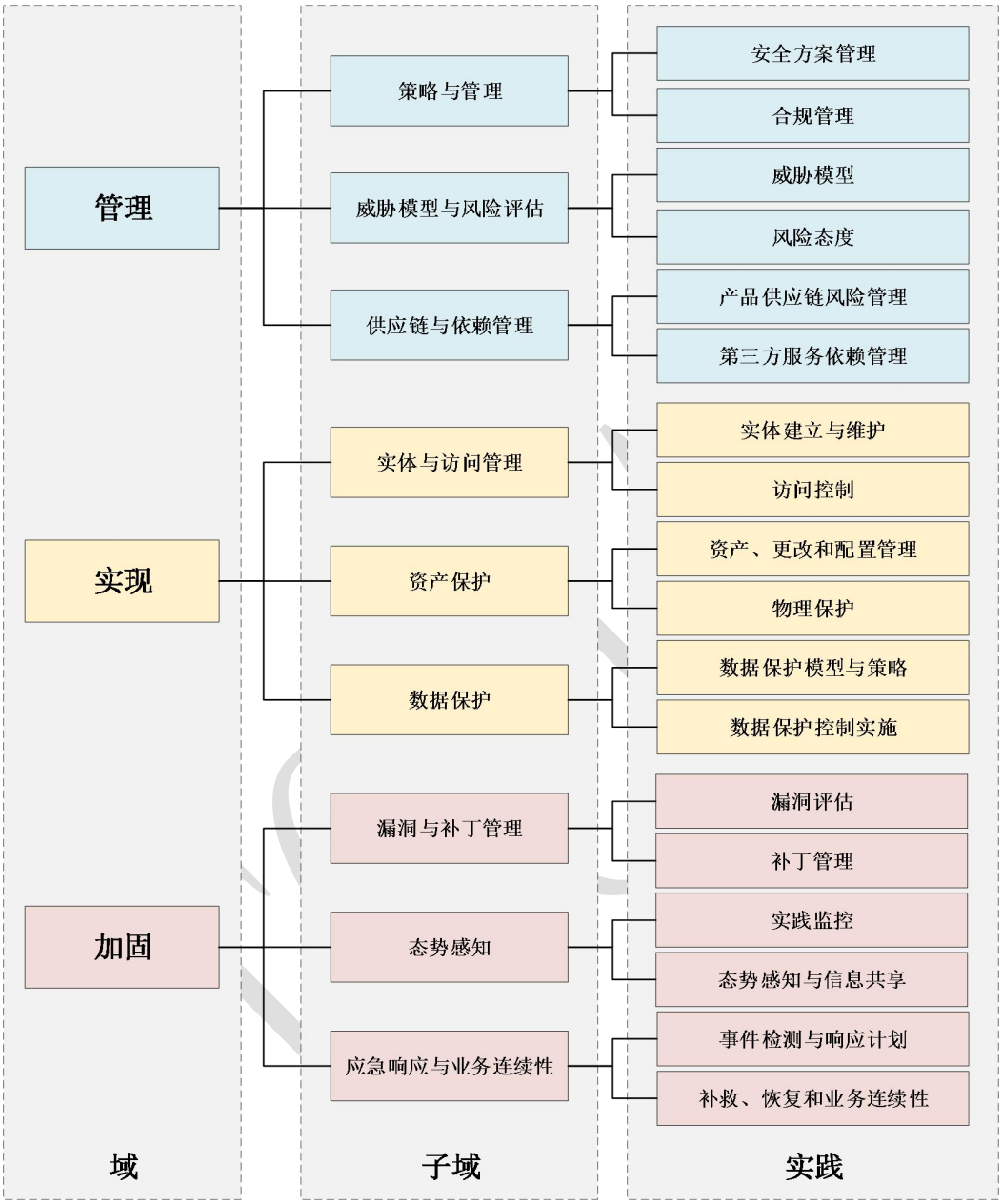

图 4- 1 物联网安全模型层次结构

安全评估有两个正交的维度：全面性和范围。全面性反映了安全实践的深度、一致性和保证程度。在模型中，全面性的使用通过综合考虑不同的方面来降低复杂性，例如组织的安全意识、实践的实施程度和实践的保证（及其演变）。例如，威胁建模的全面性等级越高，就意味着越自动化、系统化和广泛的方法。范围反映了对行业或系统需求的适应程度。这体现了支持安全成熟度域、子域或实践的安全措施的定制程度。这种定制通常需要解决物联网系统的特定行业或特定系统的限制。全面性和范围有助于对安全成熟度实践进行评分和优先级排序，而系统的安全成熟度应根据最符合其目的和预期用途的要求来确定。

4.3.2 全面性等级

每个安全域、子域和实践都有五个全面性等级，从 0 级到 4 级，数字越大表示全面性程度越高。每一个全面性等级都涵盖了较低等级的所有要求，并以额外的要求进行了扩充。

第 0 级，无：对如何应用安全实践没有共同的理解，也没有实施相关的要求（由于该级别没有应用任何保证或实践，不作进一步讨论）。

第 1 级，最低：实施了安全实践的最低要求。没有针对安全实践实施的保证活动。

第 2 级，临时：该实践的要求涵盖了主要用例和类似环境中的知名安全事件。这些要求提高了所考虑的环境的准确性和颗粒度等级。保证措施支持对实践实施的特别审查，以确保已知风险的基线缓解措施。对于这种保证，可以应用从其他成功的参考资料中学到的措施。

第 3 级，一致：要求考虑最佳实践、标准、法规、分类、软件和其他工具。这些工具为实践部署建立了一致的方法。实施的保证根据安全模式验证实施，从开始便考虑安全性以及已知的保护方法和机制进行设计。

第 4 级，正规：完善流程构成实践实施的基础，提供持续的支持和安全增强。实施的保证集中在对安全需求的覆盖，以及及时解决相关系统威胁问题。

4.3.3 范围级别

每个安全等级都有三个范围级别，从 1 级到 3 级，数字越大表示范围越窄，越具体。

第 1 级，一般：这是最广泛的范围。安全实践是在计算机系统和网络中实施的，没有对其与具体部门、使用的设备、软件或要维护的流程的相关性进行任何评估。安全能力和技术被与典型环境中相同。

第 2 级，特定行业：范围从一般情况缩小到特定行业的情况。安全实践的实施考虑了特定行业的问题，特别是容易受到某些类型攻击的组件和流程，以及已知的漏洞和已发生的安全事件。

第 3 级，系统特定：这是最窄的范围。安全实践的实施与所考虑系统的特定组织需求和风险相一致，确定了信任边界、组件、技术、流程和使用场景。

4.3.4 模板

表格 4- 1 是实践表模板。对于每个全面性级别，该表描述了目标和通用考虑因素。通用考虑因素包括：对该级别的描述、为达到该级别需要做什么、成绩指标，以帮助评估员确定组织是否达到了该级别的要求。

表格 4- 1 安全评估模型表模板

<实践名>				
<实践描述>				
	全面性等级 1（最小）	**全面性等级 2（临时）**	**全面性等级 3（一致）**	**全面性等级 4（正规）**
目标	目标描述	目标描述	目标描述	目标描述
通用考虑因素	等级描述	等级描述	等级描述	等级描述
	为达到这一级别需要做什么 考虑因素	**为达到这一级别需要做什么** 考虑因素	**为达到这一级别需要做什么** 考虑因素	**为达到这一级别需要做什么** 考虑因素
	成绩的指标 考虑因素	**成绩的指标** 考虑因素	**成绩的指标** 考虑因素	**成绩的指标** 考虑因素

安全评估模型可以以几种方式扩展。每个实践的范围可以按行业、系统或两者进行扩展。此外，随着时间的推移，该模型可以通过增加新的子域和实践来扩展。

4.4 模型应用

组织首先建立成熟度目标。业务层的相关人员使用某种形式的业务目标调查表来定义目标。技术层的相关人员根据他们对系统的理解，将这些目标转化为更详细的安全要求。一旦创建了目标或确定了相关的行业概况，组织就会进行评估以掌握当前的安全成熟度状态。可以比较目标状态和当前状态的安全成熟度，以确定差距和改进机会。在差距分析的基础上，业务和技术相关人员可以建立一个路线图，采取行动，并衡量进展。在实施改进后，组织可以进行另一次评估。这个循环反复进行，以确保在不断变化的威胁环境中始终保持适当的安全目标。

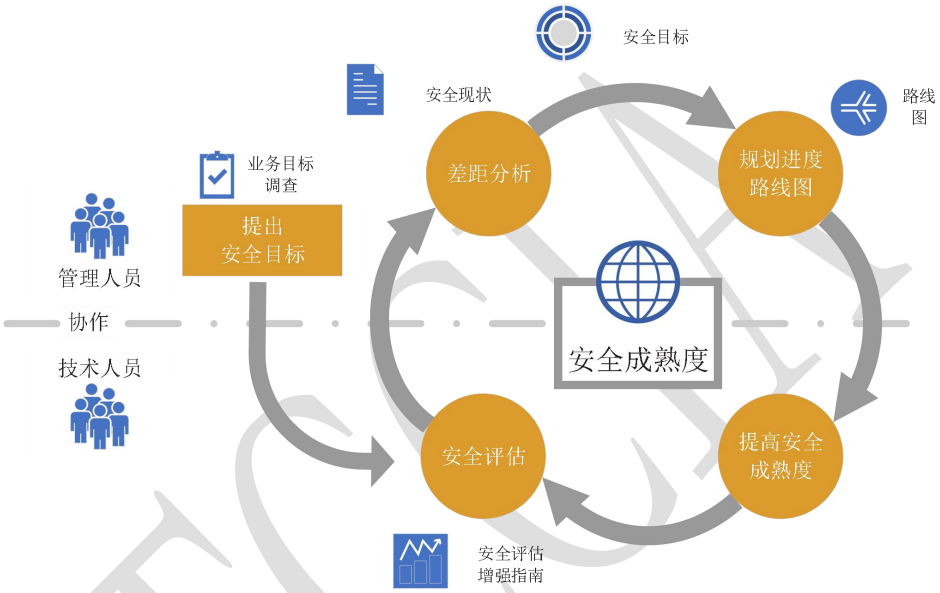

图 4- 2 工业物联网安全评估模型流程

4.4.1 内容建立

在创建安全成熟度目标或进行评估之前，重要的是建立活动的内容。首先，需要确定评估是针对一个完整的端到端系统，还是一个子系统，云或边缘，或一个网关设备？被评估的组织是解决方案提供商、最终用户还是设备或物联网平台的供应商？根据不同的背景，一些实践可能不相关，应标记为不适用。

4.4.2 创建安全目标

安全目标为系统建立初始目标安全成熟度状态。该目标包括一系列一致安全实践，让所有相关人员了解一般安全目标和每个安全实践的目的。一旦有了安全目标，它便可以在安全评估模型的后续应用中使用，以创建目标配置或评估当前的安全状态。对于特定类型的组织或系统来说，有一个安全目标配置作为特定配置是非常有用的。使用安全目标配置文件可以简化为普通用例建立目标的过程。

大多数设备、网络和系统并不要求每个安全域、子域或实践的最高全面性和范围级别。系统的安全目标被定义为每个安全成熟度域、子域和实践的全面性和范围的所有理想值的集合。

4.4.3 确定全面性等级

根据在目标安全成熟度状态中的作用的整体愿景，为每个安全域的管理、实现和加固确立目标。根据总体目标确定每个域的目标。从这组目标中选择的目标决定了整个域的最低全面性和范围等级。在该域内考虑的安全成熟度子域和实践将在此步骤中继承这些级别。这第一步提供了安全成熟度目标的粗略定义。

通过继承安全评估模型等级结构中下一级的全面性和范围级别，可以获得粗略的安全成熟度目标，以此，子域可获得与上级域相同的全面性级别，以及可得到与上级子域相同的全面性等级。

为了得到一个详细的安全目标，考虑将域的既定级别作为子域的基础等级。然后考虑每个域的安全子域所涵盖的需求。这些需求包括威胁和威胁形势的持续变化、合规性需求和监管部门的要求。前面的步骤提供了域的初始全面性和范围级别。这一步指定了是否有特定的安全相关需求，需要在既定的基线之外予以关注。

为了获得详细的安全目标，考虑将应用子域的初始等级的既定等级作为其实践的基础等级。如果实践等级被改变为更高或更低的值，这可能会影响子域的等级。

由于子域的优先级强调的是具体的安全需求，因此实践的优先级澄清了实践如何解决这些需求。有些实践可能是完全适用的，有些只是部分适用。每个实践的目标全面性和范围级别反映了覆盖子域需求的保证等级。

4.4.4 确定范围

检查每个安全域是否有跨行业的具体要求。如果是的话，将行业特定级别分配给该域和基础子域及实践。描述该域的行业特定要求，它们的来源以及应用方式。

检查每个安全域是否在几个行业中都有特定的要求，或者只针对系统。如果是，就把系统特定的级别适当地分配给该域和基础子域及实践。描述该域的系统特定要求，它们的来源以及应用方式。

对于每个子域，如果没有对父域进行修改，检查该子域是否有跨行业的特定要求。如果是，将行业特定级别分配给子域和基础实践。描述子域的行业特定要求，它们的来源以及它们的应用方式。

对于每个子域，如果没有对父域进行修改，则检查该子域是否有跨越几个行业的具体要求，或者只对系统有要求。如果是的话，给子域和基础实践分配系统特定的级别。描述子域的系统特定要求，它们的来源以及应用方式。

如果子域范围被改变为一个较高或较低的值，这可能会影响到域范围的值。

对于每个实践，如果没有对父子域进行修改，则检查该实践是否在整个行业内有具体的实施。如果是，则为该实践指定行业特定级别。描述该实践实施的行业特定要求，它们的来源以及应用方式。否则，具体说明该实践实施的行业特定要求，这些要求的来源以及应用方式。

对于每个实践，如果没有对父子领域进行修改，则检查该实践的实施是否构成了跨几个行业的具体要求，或者只对系统构成了具体要求。如果是这样，就把系统特定的级别分配给该实践。描述该实践实施的系统特定要求，它们的来源以及应用方式。否则，说明该实践实施的系统特定要求，这些要求的来源以及应用方式。

如果实践范围被改变为更高或更低的值，这可能会影响子域范围的值。

4.4.5 检查安全目标一致性

由于安全评估模型为安全实践定义了一个层次结构，有利于清晰、合理地表示这些实践的优先级，因此应根据该模型验证安全目标的一致性。如果目标不一致，那么在确定优先次序和绘制路线图时就会面临挑战。

验证包括以下检查：

根据实际需求和目的定义来验证子域和实践。在根据上级域或子域的级别为子域和实践分配全面性和范围级别的情况下，进行这种检查。相关人员将描述组织的目标安全状态的目标、需求和目的定义放在一起，并对其进行审查，在需要时进行修改。对于每一个变化，考虑该变化是否对应于相同的级别，或者是否增加该子域或实践的级别。在进行后续一致性检查的同时，可以降低级别。

检查目标全面性定义的一致性。为子域定义的任何全面性等级必须等于或大于为上级域设定的等级。为实践定义的任何全面性等级必须等于或大于为上级子域设置的等级。如果检查没有通过，则适当降低上级域或子域的级别。底层子域和实践的级别保持其值。

检查目标范围定义的一致性。子域的任何定义的范围必须等于或比为上级子域设置的级别更具体。为实践定义的任何范围必须等于或比为上级子域设置的级别更具体。如果检查没有通过，则适当降低上级域或子域的级别。底层子域和实践的级别保持其值。

如果一个子域的全面性被确定为比其继承值更高的级别，那么该域就达到了最初设定的基本级别 ″+″。(″+″表示从最初的继承值中发生了变化，并且与领域基础值不同)。除非它的所有子域都被标记为更高的级别，否则该域不会移动到更高的级别。如果子域的任何元素不能满足更高等级的要求，那么它将被视为处于较低等级，并且域本身将被降低，并被视为具有 ″+″标识的较低等级。如果所有的子域都在同一个较低等级，那么域也必须被降低到较低等级以保持一致性。

如果一个子域范围被确定为处于比其继承值更高的级别，那么该域被认为已经达到了最初设定的基本级别 ″+″。只有当它的所有子域都被标记为更高等级时，该域才会移动到更高等级。如果子域被认为处于较低的等级，则该域必须被降低，并被视为较低等级的 ″+″。如果所有的子域都在同一个较低的级别，域也必须被降低到较低的级别以保持一致性。

如果一个实践的全面性被确定为处于比其继承值更高的等级，那么该子域被认为已经达到了最初设定的基本等级，并标有 ″+″的指标以提醒其发生变化。除非子域的所有实践都被标记为更高的等级，否则子域不会移动到更高的等级。如果实践被认为处于较低等级，子域必须降低，并被认为是较低等级的 ″+″。如果所有的实践都在同一个较低等级，那么子域也必须被降低到较低等级，以保持一致性。

如果一个实践范围被确定为处于比其继承值更高的等级，那么该子域就被认为达到了最初设定的基本等级 ″+″。当子域的所有实践都被标记为更高的级别时，子域就会移动到更高的级别。如果实践被认为处于较低的等级，子域也必须被降低，并被认为是较低的等级 ″+″。如果所有的实践都在同一个较低的级别，子域也必须被降低到较低的级别以保持一致性。

一致性检查必须在层次结构中流动，以确定子域等级的变化是否影响到它们上面的域的值。

5 模型实施分析

本章节将从技术、管理、工程三个维度详细分析模型的设计。

5.1 技术实现

5.1.1 实体识别

识别从技术上确保工业物联网的关键实体。

关键实体是对工业物联网生产环节至关重要的、并且可能不是项目现成可用的资源。关键资源可能包括具有特殊技能的人员、工具、设施、或数据。关键资源可以通过分析项目任务和进度，以及与类似项目对比来识别。

实践示例：检查项目进度并且设想每个时间点所要求的资源的类型。列出不容易获得的资源列表。通过设想为合成系统和工作产品所要求的工程技能，检查和补充这个列表。

5.1.2 资源访问管理

通过对数据导入、导出过程中对数据的安全性的管理，防止相关过程中可能对数据自身的可用性和完整性构成的危害、以及可能会存在的数据泄漏风险。

a） 建立数据导入导出审核流程的在线平台，组织机构内部的对数据导入导出可通过平台进行审核并详细记录，确保没有超出服务提供者的数据授权使用范围。

b） 建立针对数据导入导出过程的安全技术方案，采用密码技术，对数据导入导出终端、用户或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的保证；采用密码技术，对关键的敏感数据在导入导出的过程采用数据加密的手段，以保证数据在导入导出过程中的保密性、完整性和可用性；对数据导入导出通道进行有效的缓存数据清除，以保证导入导出过程中涉及的数据不会被恶意恢复。

c） 针对数据导入导出的日志建立相应的管理和审计方案，以保证对对导入导出过程中的相关日志信息的有效记录，采用密码技术，以保证相关日志的存储完整性保护，并通过定期的审计工作开展发现其中存在的安全风险。

d） 在组织机构统一的对数据导入导出的原则和规范要求下，采取密码技术和多因素鉴别技术对数据导入导出操作员进行身份鉴别，为数据导入导出通道提供冗余备份能力，确保数据安全可靠导入导出要求；对数据导入导出接口进行流量过载监控，确保海量数据导入过程安全可控。

e） 组织机构在数据导入导出审核平台上对各类审核流程中应关注的安全风险进行提示，以辅助审核人员进行风险的评估，提升审核的准确度和效率；配置专业数据导入机制或服务组件，明确数据导入导出最低安全防护基线要求。

5.1.3 数据存储安全

通过基于组织机构的数据量增长、数据存储安全需求和合规性要求制定适当的对存储架构，以实现对存储数据的有效保护。

a） 建立可伸缩数据存储架构，以满足数据量持续增长、数据分类分级存储等需求。该数据存储架构提供对个人信息、重要数据等加密存储能力，并具备数据存储跨机柜或跨机房容错部署能力。

b） 统一提供有效的技术方案，对数据存储完整性和多副本一致性真实进行检测和恢复。

c） 建立有效的数据加密工具，并提供有效的密钥管理机制已实现对密钥的全生命周期（存储、使用、分发、更新和销毁）的安全管理。

d） 确保存储架构具备数据存储跨地域的容灾能力。

e） 建立满足应用层、数据平台层、操作系统层、数据存储层等不同层次的数据存储加密需求的数据存储加密架构。

f） 组织机构提供固定的数据加密模块供存储功能的开发人员调用，该模块可自动识别数据的类型和级别进行数据加密处理，从而保证数据的加密功能的统一性。

5.1.4 网络安全

物联网的网络部分包含通信网、互联网、行业专网等，具有网络异构化、多样化等特点，其安全要求主要包含接入安全和通信安全。

对于接入安全，需要符合以下清单：

a）各类感知终端和接入设备在接入网络时应具备唯一标识；

b）应采用密码技术，对各类感知终端接入行为进行身份鉴别；

c）对于网络的访问控制采取禁用闲置端口、设置访问控制策略等防护手段

d）对于网关、防火墙等网络边界设备，需配置安全策略，具备加密功能和访问控制等防护措施；

对于通信安全，需要符合以下清单：

a）物联网中的数据传输协议需有数据校验功能以确保数据传输的完整性；

b）应采用标准化时间戳机制等技术确保数据传输的可用性；

c）应采用密码技术对数据传输的隐私性进行保护；

d）在网络数据交互前，应采用密码技术为交互双方身份的可信性提供证明；

e）可采用国家政策允许的加密算法对网络传输数据进行加密，确保信息的保密性；

f）物联网应具备防伪基站攻击、网络接力攻击的能力。

5.2 管理安全控制

5.2.1 安全管理方案

物联网是由多个子系统组成的复杂系统，其运行和维护通常由不同责任方负责开展，其安全要求包括：

a）物联网中不同责任方应根据其职责，在物联网系统建设时，对物联网设备和系统的获取做出规定，如规定设备和系统提供方的资质要求、可信赖性等、提供系统文档的详细程度，供应链的安全要求等；

b）对于物联网系统运行维护中的相关参与人员，应提出人员资质、身份审核、可信证明、诚信承诺等要求，以确保其在物联网系统维护过程中的安全可信；

c）应对物联网系统运维的时效性、维护工具等提出安全要求，对于远程维护设备的，应对远程维护制定安全守则。

5.2.2 管理团队安全能力建设

a） 制定信息系统资产的安全管理制度，明确信息系统资产安全管理目标和安全原则、信息系统资产的全生命周期管理要求、资产登记要求和分类标记要求，并针对安全管理制度执行定期审核和更新。

b） 建立信息系统资产建设和运营管理制度和机制，明确规划、设计、采购、开发、运行、维护及报废等资产管理过程的安全要求。

c） 建立组织机构内的信息系统资产登记机制，形成整体的信息系统软硬件资产清单，明确系统资产安全责任主体及相关方，并及时更新系统资产相关信息。

d） 建立和实施信息系统资产分类和标记规程，使资产标记易于填写和依附在相应的系统资产上。

e） 建立信息系统资产更新、运营风险评估和供应链安全审查规程和制度。

5.3 工程控制与维护

5.3.1 业务规划与管理

对于工业物联网中的新业务开发和上线流程，一定要遵循标准开发流程和审查流程。

开发模型有如下几种：

a） 瀑布模型

b） 原型模型

c） 演化模型

d） 螺旋模型

e） 增量模型

f） 喷泉模型

g） 构建组装模型

上述模型根据实际情况选其一即可，不应随意更换。开发的过程中一定要遵循每个步骤的规定，列出开发流程图，确定当前所处的时间节点，确保不会遗漏步骤。

5.3.2 工程评审

工业物联网是重要的工业生产基础，对所有的新业务上线、业务基线变更、硬件设施更新等操作都要经过评审。评审分为准备、会议、结论、修改跟踪与审核步骤。以下步骤是一个工程评审运作模板，需根据实际情况确定评审规范、附带文件模板、流程等。

(1) 评审准备

a） 项目经理把该阶段完成的工作成果提交给质量保证工程师，提出评审申请；质量保证工程师编写评审记录经部门经理确认后方可进行评审会议。

b） 项目经理根据项目的特征组建相应的评审会成员，并确定评审会议主持人、会议记录人。

c） 质量保证工程师确定评审会议的时间、地点和参加会议的人员（包括评审员、记录员、用户），然后提前通知所有相关人员。

d） 质量保证工程师将需要评审的工作成果提前 X 天发给评审员，评审员在进行正式评审会议之前应了解所需评审的工作成果发送至项目质量保证工程师、抄送项目经理。

(2) 评审会议

a） 评审主持人介绍本次评审会议的议程、重点、原则、时间限制等。

b） 评审成员在评审记录上签名。

c） 工作成果的作者或项目经理简要介绍本阶段工作成果内容。各评审员提出疑问，工作成果的作者回答评审员的问题。双方应当对有争议的问题达成一致的处理意见。对于当场难以解决的问题，由主持人决定“是否有必要继续讨论”或者“另定时间再讨论”。

d） 评审会议的记录员应对会议中的每个有争议的问题进行记录。

e） 评审小组给出评审结论和意见，确定是否可转入下一阶段工作，主持人签字后，本次会议结束。

(3) 评审结论

评审的结论包括三种，分别是通过、原则通过、未通过：

a） 通过。不需要修改。把该阶段产生的工作成果配置项交由配置管理人员放入受控库中进行版本控制，软件开发可以转入下一阶段工作。

b） 原则通过。稍作修改。需做少量的修改，之后通过审核即可转入下一阶段工作。

c） 未通过。软件开发项目组重新做该阶段的工作后，再提出评审申请，质量保证工程师组织人员重新进行评审。

(4) 修改跟踪与审核

由项目经理督促工作成果的作者修改工作成果，消除已发现的缺陷。

项目组或工作成果作者根据评审意见，对工作成果实施更改并在评审记录中填写修改情况，由部门经理或项目负责人跟踪修改结果并签字审核确认。修改完成后在部门经理认可的情况下转入下一阶段的工作。

消除所有已经发现的缺陷后，再将修改后的工作成果提交给部门经理（或者指定审核人）审核。

由部门经理（或者指定审核人）审核修改后的工作成果。审核结论有两种：

a） 修改后的工作成果合格，可以进入下一阶段的工作。完善后的文档交由配置管理人员进行版本控制

b） 修改后的工作成果仍然不合格，需重新修改，重复“修改跟踪与审核”工作。

5.3.3 业务运行维护

a） 物联网系统在运行过程中，各子系统责任方应结合自身要求，制定安全管理策略规程；

b）应明确物联网系统不同设备责任人安全职责及其行为准则；

c）根据实际情况制定应急计划和配置管理策略；

d）必要时，可对物联网系统定期开展安全评估等工作，安全评估可参照工业物联网评价机制。

6 安全评估

当前安全状态是指特定系统已实施的安全实践的当前状态，其格式与安全目标类似。通常情况下，安全评估通过技术测试或渗透测试评估控制的有效性，通过审计控制来评估每个安全实践。然后可以将其与目标状态进行比较，以便找出差距，并产生一个实现目标状态的路线图。

确定当前的安全状态：

确定评估的范围： 选项包括整个组织、仅组织的选定部分，或仅特定的安全实践。对于要评估的每个安全实践，应该包括哪些相关人员，以及应该评估哪些已实施的控制？如果不能包括相关人员或不能在合理的时间内评估特定的控制措施，是否有其他途径可以评估其安全？

确定评估方法：考虑的因素包括：

- 审查是由内部团队还是由第三方进行？
- 测试方法是否包括策略审查、访谈、审计和渗透测试？
- 将使用什么框架来列举和评估可能的控制？

注重评估控制的真正有效性的测试可以提供更准确的安全状况，但也往往更耗费时间。所需的专业知识也可能不存在于内部。

相关人员的准备： 准备工作增加了在合理时间内完成评估的可能性，并且评估的最终结果是准确的。应该：

- 确定相关人员和联络点、
- 让那些没有参与计划的相关人员了解评估和它的目标、
- 为评估小组安排与相关人员的访谈、
- 收集相关策略、文件、合同、以前的评估报告等、
- 准备渗透测试所需的任何访问，如网络访问和域证书等。

评估： 准备工作完成后，评估小组应审查已实施的安全实践。

报告： 评估小组应该将他们的发现记录在一份正式的报告中，提交给商业决策者和其他相关的相关人员。它应该通过组织的特定行业和业务情况来解释团队的发现。它应该解决每个安全实践及其相关的控制措施和低等级的细节。它可能包括一个对每个控制和实践进行打分或测量的系统，以便为组织提供相对优先级、随时间变化和其他比较的衡量标准。

6.1 评估等级

当组织满足了一个全面性等级的所有指标时，便达到了该等级的要求。

全面性等级之间的过渡取决于明确记录特定等级的特点和要求。

- 对于最小的全面性等级，定义实践实施目标和适当的最小措施。
- 对于临时全面性等级，描述用例和支持这些用例所需的基线措施。
- 对于一致全面性等级，记录公认的最佳实践、标准、法规和适用的支持工具。
- 对于正规全面性等级，记录支持性的流程定义。

范围级别之间的过渡由安全成熟度目标定义期间确定的部门特定问题和系统特定需求和风险决定。

因此，在安全成熟度评估之前，相关人员必须就全面性和范围级别的确切定义达成一致，如图 6- 3 所示。

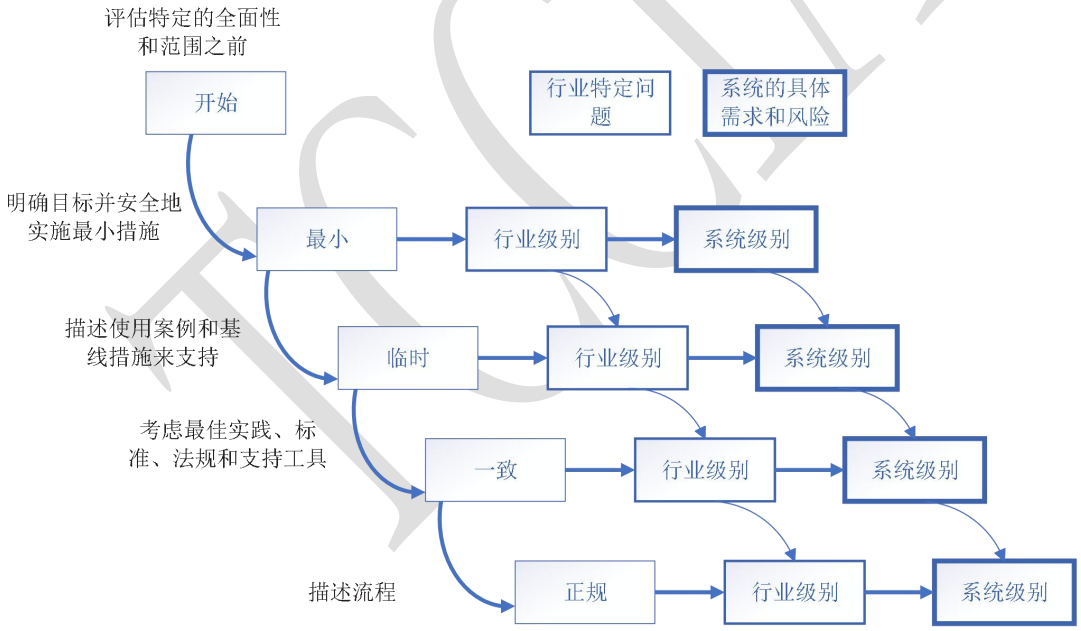

图 6- 3 安全实践的全面性和范围级别之间的状态和转换

一些组织需要展示证明一些（不是所有）更高等级要求的项目。例如，如果一个组织满足了 2 级的所有条件，但只满足了 3 级的部分条件，他们可以被视为 2+级；但他们需要满足 3 级的所有条件才能被视为 3 级。同样，如果一个组织满足了 1 级的所有项目，2 级的 90%和 3 级的一些项目，他们将被认定为 1+级。

在实践层面，描述一个组织离实现下一个级别有多远可能是有用的，相关人员需要知道达到该级别的付出程度。在这种情况下，评估者可以使用 “2.1”或 “2.8 ”这样的数字来描述评估结果。由于每个案例的背景可能不同，可能需要不同的机制。

与目标等级设定可继承不同的是，现状评估是通过对实践的详细评估自下而上进行的。一个子域是由其实践的最低级别来确定的。如果实践有不同的级别，子域就被标识为最低级别的 “+”，以表明应该查看这些实践以了解内容。除非子域的所有实践都被标记为更高的级别，否则子域不会移到更高的级别。在全面性的情况下，如果一些实践在 2 级以上，可以被指定为 2+；在范围的情况下，如果一些范围在系统范围级别，可以指定为“行业+”。在子域层面上对实践等级进行平均化是无效的，除非对实践进行探讨。

一旦为子域设定了数值，就可以在域的层面上进行类似的总结和检查。如果子域有不同的全面性等级，那么该域就被确定为最低的子域全面性等级，并加上 “+”，以表示应该查看子域和实践以了解内容。除非其所有的子域都被标记为更高的级别，否则该域不会移到更高的级别。在全面性的情况下，如果一些子域在 2 级以上，可以指定为 2+级；在范围的情况下，如果一些范围在系统范围级别，可以指定为 “行业+”。与子域级上的实践值类似，在域级上对子域等级进行平均化是无效的，除非对实践进行探讨。

6.2 差距分析

有了目标状态和当前状态，组织可以进行差距分析，以确定安全改进和发展的适当域。对于那些在两种状态之间存在差异的控制，需注意差距大小以帮助在路线图中确定优先次序。同时，也要注意特定的控制可能没有达到目标状态的任何情况，但随之而来的潜在风险被另一个控制所缓解了。这个过程应该产生一个未达到目标状态的安全控制清单，这些控制的当前状态和目标状态之间的差距，以及任何可能通过其他方式缓解风险的控制的说明。

基于目标状态和当前状态之间的比较，业务和技术相关人员可以衡量进展并协商安全成熟度提升的步骤。

6.3 规划路线图

利用差距分析的结果可建立一个未来安全改进的路线图。路线图根据确定的差距、主要的业务和安全需求及关注点、可用的资源和专业知识以及公认的业务实践来确定活动的优先次序。

安全成熟度可以通过提高全面性和转移范围来加强。如果其中一个方面不需要改进，可以计划和执行改进另一个方面的步骤。如果全面性和范围都需要改进，相关人员应该考虑全面性和范围对该实践的相对重要性，以及先改进一个再改进另一个的可能性。对于当前状态与目标有差距的每项实践：

- 识别由于安全、监管、法律、道德或合同义务而应立即改善的全面性、
- 确定哪些地方因类似原因应立即改善范围、
- 确定哪些补救措施可以达到目标状态。使用最佳实践指南来确定最有效的控制改进措施、
- 根据安全、监管、法律、道德或合同义务，对补救措施进行优先排序。

对于每个潜在的补救措施，确定其在金钱和组织资源方面的成本。阐明补救措施的效果以及由此产生的安全改进。

制定一个安全改进的路线图。路线图应优先考虑满足法律或监管要求的补救措施，以及那些能以最低成本带来最大改进的补救措施。制定路线图时的其他考虑包括

- 安全控制之间可能存在的依赖关系、
- 可能影响多个控制的改进、
- 实施每个补救措施所需的时间和资源、
- 在一个已实施的变更完全有效之前所需的时间和资源。

然后为每个补救项目确立所有权、里程碑和最后期限。

差距分析有助于组织制定一个路线图，以改善其安全态势和成熟度。了解差距可以使组织了解不同安全要求和控制的相对优先级。该模型确定了实现某种程度的全面性和范围所需的条件。

6.4 持续改进

如图 6- 4 显示了物联网安全评估度模型过程。一个持久的系统安全状态只有通过持续的安全评估和改进才能实现，并随着时间的推移进行协调。因此，我们在一个 "计划-执行-检查-行动 "的循环中进行迭代（行动指如果对改进步骤的结果检查成功，则接受新的基线）。这个循环从为特定系统建立安全成熟度的目标开始。然后，如图 6- 4 所示，开始了安全改进的高层次迭代过程。安全威胁的变化速度和减轻威胁的方法决定了执行该周期的频率。

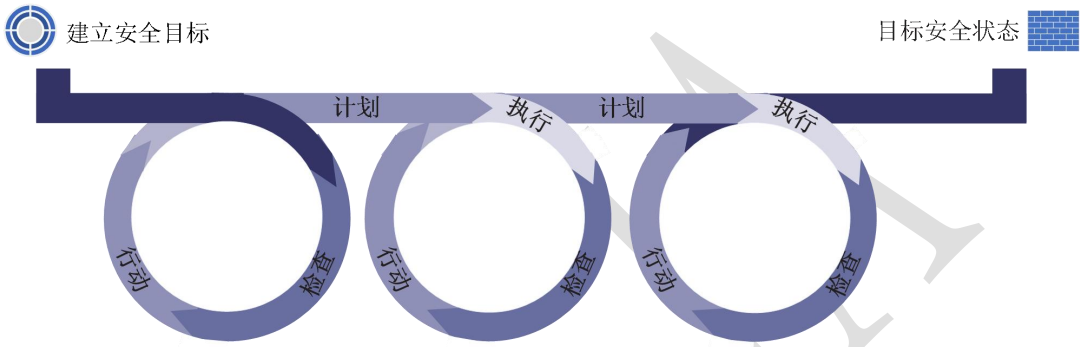

图 6- 4 安全评估模型改进周期