变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2021.3	吕萍/2021.3	

物联网安全拓展要求（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
感知节点设备物理防护	a)感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压，强振动	许多感知节点资源受限，成本低廉，可能散布在无人职守的区域，如果所处物理环境对感知节点设备造成物理破坏，将会导致感知节点无法正常工作，并很难及时发现	1)核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致 2)核查感知节点设备所处物理环境是否采取了防挤压、防强振动的防护措	1)感知节点设备所处物理环境的设计或验收文档明确了感知节点设备所处物理环境的防物理破坏要侧如具有防挤压、防强振动等的说明。 2)感知节点设备所处物理环境采取了防物理破坏的相应防护措施，例如，室外监控摄像机的外部安装需要在建筑物的外墙上安装孔和支架，并注意避免强烈撞击	符合情况：感知节点放置固定在XXX，具有防风、防雨、防火、防挤压、防强振动能力。 部分符合情况：无 不符合情况：感知节点放置在XXX，未进行相应的安全防护。
	b)感知节点设备在工作状态所处物理环境应能正确反应环境状态(如温湿度传感器不能安装在阳光直射区域)	避免感知节点设备所处物理环境错误，导致采集到错误信息或采集不到信息	1)核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致 2)核查感知节点设备所处物理环境是否能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)	1)感知节点设备所处物理环境的设计或验收文档明确了感知节点设备在工作状态所处物理环境的说明 2)感知节点设备所处物理环境能正确反映环境状态，例如温湿度传感器不能安装在阳光直射区域，监控摄像机的镜头不要对准强光处	符合情况：感知节点放置在XXXX，周围环境能够保证感知节点正常运行使用。 部分符合情况：无 不符合情况：感知节点安装位置在XXXX，周围环境影响感知节点正常使用。
	c)感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等	感知节点资源有限，常采用短距离无线通信方式，如果所处环境存在强干扰阻挡屏蔽等情况，容易导致感知节点无法传输信息	1)核查感知节点设备所处物理境的设计或验收文档，是否有感知节点设备所处物理环境防强干扰，防阻挡屏蔽等能力说明，是否与实际情况一致 2)核查感知节点设备所处物理环境是否采取了防强干扰，防阻挡屏蔽等能防护措施	1）感知节点设备所处物理环境的设过或验收文档有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明。例如，红外摄像机安装位置应该避免潮湿、多尘、强电磁辐的场所 2)感知节点设备所处物理环境采取了防强干扰，防阻挡屏蔽等能措施。例如，室外监控摄像机探头如果经常会遇上热气而起雾，考虑安装镜头除雾器；如果监控摄像机探头安装在玻璃后面，要确保镜头靠近玻璃(如果距离太远，玻璃容易反射图像)	符合情况：感知节点设备所处物理环境采取了防强干扰，防阻挡屏蔽等能措施。如室外监控摄像机探头安装镜头除雾器。 部分符合情况：无 不符合情况：感知节点设备所处位置未采取防抢干扰、防屏蔽等措施。
	d)关键感知节点设备应具有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应)	感知节点和网关节点设备往往24小时开机，无专人职守，如果关键感知节点没有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应），将会因电力耗尽而无法正常工作	1)核查关键感知节点设备(关键网关节点设备)电力供应设计或验收文档，是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施(关键网关节点设备持久稳定的电力供应措施) 2)核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致	1)关键感知节点设备(关键网关节点设备)电力供应设计或验收文档标明了电力供应要求，其中明确了保障关键感知节点设备长时间工作的电力供应措施(关键网关节点设备持久稳定的电力供应措施).例如，监控摄像机交流电压适应范围一般是200-240V,抗电源电压变化能力较弱，在系统中使用时需要添加稳压电源 2)核查相关电力供应措施的运行维护记录，确保与电力供应设计一致	符合情况：感知节点网关设备具有持续的电力供应措施，并安排专人定期检查电力情况。 部分符合情况：感知节点网关设备具有持续的电力供应措施，未定期检查电力供应情况。 不符合情况：感知节点网关设备未具有持续的电力供应措施。

接入控制	应保证只有授权的感知节点可以接入	感知节点数量巨大，无专人职守，这些设备可能被劫持或物理破坏，然后非法节点伪装成客户端或者应用服务器发送数据信息、执行操作，因此需要对感知节点进行标识和鉴别，以保证只有授权的感知节点可以接入	1)核查感知节点接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述 2)对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法	1)感知节点接入机制设计文档包括了防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述。通常采用各类感知终端和接入设备在接入网络时设备唯一标识，并禁用闲置端口、设置访问控制策略等防护手段。例如，在视频专网中部署视频接入安全管理系统，对摄像机及其它前端IP设备进行品牌、型号、IP, MAC等绑定，并进行准入策略管控，只有通过认证的设备才允许接入 2)对边界和感知层网络进行渗透测试，不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法	符合情况：通过网关设备对感知节点进行授权控制，对感知节点设备信息进行记录绑定。 部分符合情况：无 不符合情况：1.无管理端对感知节点设备进行管控。2.存在绕过白名单、身份认证的漏洞。
入侵防范	a)应能够限制与感知节点通信的目标地址，以避免陌生地址的攻击行为	对感知节点通信的目标地址进行限制，防止被攻击后参与DDOS攻击或成为攻击跳板	1)核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施 2)核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施 3)对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击	1)感知层安全设计文档有对感知节点通信目标地址的控制措施说明。例如，在网络摄像机的汇聚交换机上划分VLAN 2)感知节点设备配置了对感知节点通信目标地址的控制措施，相关配置参数符合设计要求。例如，在汇聚交换机上划分VLAN,在汇聚交换机的接口上配置相关的VLAN数据 3)对感知节点设备进行渗透测试，能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击	符合情况：在网络摄像机的汇聚交换机上划分VLAN，相关配置参数符合设计要求。 部分符合情况：无 不符合情况：未采取措施限制与感知节点通信的目标地址。
	b)应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为	对网关节点通信目标地址进行限制，防止被攻陷后参与DDOS攻击或成为攻击跳板	1)核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明 2)核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关配置参数是否符合设计要求 3)对网关节点设备进行渗透测试，能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击	1)感知层安全设计文档有对网关节点通信目标地址的控制说明。例如，通过防火墙或配置交换机VLAN对网关节点通信目标地址进行控制 2)网关节点设备配置了对网关节点通信目标地址的控制措施，相关配置参数符合设计要求。例如，相关防火墙或交换机VLAN的配置参数符合设计要求 3)对网关节点设备进行渗透测试，能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击	符合情况：通过防火墙或配置交换机VLAN对网关节点通信目标地址进行控制，相关配置参数符合设计要求。 部分符合情况：无 不符合情况:未通过安全防护设备对通信的目标地址进行识别。

感知节点设备安全	a)应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更	感知节点设备数量巨大，往往在线批量进行软件应用配置或变更，如果没有采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更，容易导致感知节点监测数据泄露或设备被非法关闭	1)核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上软件应用进行配置或变更 2)通过试图接入和控制传感网访问未末授权的资源，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效	1）感知节点设备采取了一定的技术手段防止非授权用户对设备上软件应用进行配置或变更，例如，给感知节点设备配置安全性强用户名和登录密码 2)感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源行为控制有效	符合情况：感知节点设备采用用户名和口令进行认证，口令满足复杂度要求，访问控制措施对非法访问和非法使用感知节点设备资源行为控制有效。 部分符合情况：感知节点设备采用用户名和口令进行认证，口令满足复杂度要求，权限未进行细化。 不符合情况：所有人员都可以对感知节点设备上的软件进行操作。
	b)应具有对其连接的网关节点设备（包括读卡器)进行身份标识和鉴别的能力	很多物联网感知节点是处在无人值守的位置，就给了攻击者可趁之机，便于从 无人值守的设备中获得用户身份等的隐秘信息，并以此设备对通信网络进行攻击，因此需要具有对其连接的网关节点设备(包括读卡器)进行身份标识和识别的能力	1)核查是否对连接的网关节点设备(包括读卡器)进行身份标识与鉴别 2)测试验证是否不存在绕过身份标识与鉴别功能的方法	1)连接的网关节点设备(包括读卡器)进行身份标识与鉴别，配置了符合安全策略的参数 2)不存在绕过身份标识与鉴别功能的方法	符合情况：连接的网关节点设备(包括读卡器)进行身份标识与鉴别，配置了符合安全策略的参数，且不存在绕过身份标识和鉴别。 部分符合情况：对连接的感知节点设备(包括读卡器)设备进行身份标识与鉴别，未配置符合安全策略的参数或者参数设置不合理。 不符合情况：1.存在绕过身份标识与鉴别功能的方法。2.未部署接入安全管理系统对节点设备进行标识和鉴别。

	c)应具有对其连接的其他感知节点设备(包括路由节点)进行身份标识和鉴别的能力	攻击者通过假冒网络中已有的感知节点或网关节点，可以监听传感网络中传输的信息，向传感网络中发布假路由信息或传送假的数据信息、进行拒绝服务攻击等。需要具有对其连接的其他感知节点设备（包括路由节点)进行身份标识和鉴别的能力	1)核查是否对某他感知节点设备(包括路由节点)设备进行身份标识与鉴别，是否配置了符合安全策略的参数 2)测试验证是否不存在绕过身份标识与鉴别功能的方法	1)对连接的某他感知节点设备(包括路由节点)设备进行身份标识与鉴别，配置了符合安全策略的参数 2)不存在绕过身份标识与鉴别功能的方法	符合情况：对连接的感知节点设备(包括路由节点)设备进行身份标识与鉴别，配置了符合安全策略的参数，且不存在绕过身份标识和鉴别。 部分符合情况：对连接的感知节点设备(包括路由节点)设备进行身份标识与鉴别，未配置符合安全策略的参数或者参数设置不合理。 不符合情况：1.未对连接的感知节点设备进行身份标识和鉴别。2.对感知节点设备进行身份鉴别，但可以被绕过。
	a)应设置最大并发连接数	由于物联网感知节点数量巨大，如果大量感知节点设备在很短时间内接入网络或向网关节点发出连接请求，而网关节点全部进行响应和连接，很可能会导致网关节点超负荷运行或宕机，需要对网关节点设备设置最大并发连接数	核查网关节点设备是否配置了最大并发连接数参数	网关节点设备配置了最大并发连接数参数	符合情况：网关节点设备配置了最大并发连接数参数。 部分符合情况：无 不符合情况：网关节点设备未配置最大并发连接数参数。
	b)应具备合法的连接设备(包括终端节点、路由节点、数据处理中心)进行标识和鉴别的能力	物联网感知层大量使用无线通信和电子标签技术，大部分为无人值守设备，使得隐私信息威胁问题非常突出。如果隐私信息被攻击者非法获取，将会给用户带来安全隐患。网关节点设备需要具备对合法连接设备(包括终端节点、路由节点、数据处理中心)进行标识和鉴别的能力，降低被攻击者非法获取隐私数据的风险	1)核查网关节点设备是否能否对连接设备(包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能 2)测试验证是否不存在绕过身份标识与鉴别功能的方法	1)网关节点设备能对连接设备(包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能；或者部署了接入安全管理系统，可以进行准入策略管控，只有通过认证的设备才允许接入 2)不存在绕过身份标识与鉴别功能的方法	符合情况：网关节点设备能对连接设备(包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能，部署了接入安全管理系统，可以进行准入策略管控，只有通过认证的设备才允许接入。 部分符合情况：无 不符合情况：1.存在绕过身份标识与鉴别功能的方法。2.未部署接入安全管理系统对节点设备进行标识和鉴别。

网关节点设备安全	c)应具备过滤非法节点和伪造节点所发送的数据的能力	攻击者通过假冒网络中已有的感知节点或网关节点，可以监听传感网络中传输的信息，向传感网络中发布假的路由信息或传送假的数据信息、进行拒绝服务攻击等。需要具备过滤非法节点和伪造节点所发送的数据的能力	1)核查是否具备过滤非法节点和伪造节点发送的数据的功能 2)测试验证是否能够过滤非法节点和伪造节点发送的数据	1)具备过滤非法节点和伪造节点发送的数据的能力。例如，部署视频专用防火墙，仅允许通行相关视频网络协议，对其他协议进行阻挡；并启动终端准入策略，根据注册终端、未注册终端、未知设备、替换设备终端类型进行不同的阻断和记录策略 2)经测试能够过滤非法节点和伪造节点发送的数据	符合情况：部署有XXX防护设备，仅允许通行相关XX协议，对其他协议进行阻挡，并启动终端准入策略，根据注册终端、未注册终端、未知设备、替换设备终端类型进行不同的阻断和记录策略。 部分符合情况：无 不符合情况：未采取措施或部署防护设备对数据进行验证和过滤。
	d)授权用户应能够在设备使用过程中对关键密钥进行在线更新	由于物联网中的感知节点和网关节点数量巨大，部署位置广泛，人工更新关键密钥则变得更加困难，因此需要提供授权用户在设备使用过程中对关键密钥进行在线更新的能力	核查感知节点设备是否对其关键密钥进行在线更新	感知节点设备支持对其关键密钥进行在线更新	符合情况：感知节点设备支持对其关键密钥进行在线更新。 部分符合情况：无 不符合情况：感知节点设备未对其关键密钥进行在线更新。
	e)授权用户应能够在设备使用过程中对关键配置参数进行在线更新	由于物联网中的感知节点和网关节点数量巨大，部署位置广泛，人工更新关配置参数则变得更加困难，因此需要提供授权用户在设备使用过程中对关键配置参数进行在线更新的能力	核查感知节点设备是否支持对其关键配置参数进行在线更新及在线更新方法是否有效	感知节点设备支持对关键配置参数进行在线更新，并且在线更新方式有效	符合情况：感知节点设备支持对关键配置参数进行在线更新，并且在线更新方式有效。 部分符合情况：无 不符合情况：感知节点设备是不支持对其关键配置参数进行在线更新
抗数据重放	a)应能够鉴别数据的新鲜性，避免历史数据的重放攻击	数据新鲜性(data freshness)是指对所接收的历史数据或超出时限的数据进行识别的特性。可以使用时间戳或计数器，提供数据新鲜性保护。在联网监控视系统中，用于防止攻击者替换监控视频(掩饰非法活动)	1)核查感知节点设备鉴别数据新鲜性的措施，是否能否避免历史数据重放 2)将感知节点设备历史数据进行重放测试，验证其保护措施是否生效	1)感知节点设备在读取或状态控制过程中具有数据传输新鲜性保护机制，如时间戳、序列号等内容。 2)将感知节点设备历史数据进行重放，感知节点设备能在读取或状态控制过程中发现时间戳、序列号或者其他新鲜性保护信息不符合要求	符合情况：感知节点设备在读取或状态控制过程中具有数据传输新鲜性保护机制，如时间戳、序列号等内容。 部分符合情况：无 不符合情况：未采取措施对数据新鲜性进行保护。

机数据重放	b)应能够鉴别历史数据的非法修改，避免数据的修改重放攻击	物联网的感知节点往往是大规模部署，并且存在大量无人值守设备，这些设备可能被劫持，攻击者通过假冒网络中已有的感知节点或网关节点，可以对历史数据进行非法修改，向传感网络中发布假的路由信息或传送假的数据信息。需要能够鉴别历史数据的非法修改，避免数据的修改重放攻击	1)核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否有必要的恢复措施 2)测试验证是否能够避免数据的修改重放攻击	1)具备对网络节点存储数据的完整性检测机制，实现鉴别信息、协议转换规则、审计记录等重要业务数据的完整性检测，具备对传输数据的完整性检测机制，实现重要业务数据传输完整性保护，例如：校验码、消息摘要和数字签名等 2)具有通信延时和中断的处理机制，经测试能够避免数据的修改重放攻击	符合情况：配备有检测感知节点设备历史数据被非法篡改的设备。 部分符合情况：无 不符合情况：未配备检测设备，无法对设备数据篡改进行检测。
数据融合处理	应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用	传感网络和通信网络是异构网络，在异构网络数据汇总时，攻击者可以利用传感网络的安全性等特点，伪造通信网络的命令指示，从而使得物联网设备断开或者做出错误的操作或响应；或诱使物联网设备向通信网络发送假冒的请求制应，从而使得通信网络做出错误的判断而影响网络安全。需要对来自传感网的改据进行数据融合处理，使不同种类的数据可以在同一个平台被使用	1)核查是否提供对来自传感网的数据进行数据融合处理的功能 2)测试验证数据融合处理功能是否能够处理不同种类的数据	1)具备对来自传感网的数据进行数据融合处理的功能，实现对感知数据、控制数据及服务关联数据的加工、处理和协同，为物联网用户提供对物理世界对象的感知和操控服务的接口 2)数据融合处理功能能够处理不同种类的数据，将感知对象和控制对象与传感网系统、标签识别系统、智能设备接口系统等以数据通信类接口或数据通类接口的方式进行关联，实现物理世界和虚拟世界的接口绑定	符合情况：通过XXX进行数据转换处理，将数据对象通过XXX平台统一展示。 部分符合情况：无 不符合情况：未对来自传感网的数据进行数据融合处理，不能够被统一平台使用。
	a)应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护	一旦感知节点设备或网关节点设备被非法关闭(或损坏),将导致相关数据无法采集。在联网监控视频系统发生该现象时，将导致非法活动不能被及时发现和追朔	1)访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长 2)核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护护人、维护设备、故障原因、维护结果等方面内容	1)有专门的人员对感知节点设备、网关节点设备进行定期维护。如果物联网的定期维护由第三方提供服务，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 2)感知节点设备、网关节点设备部署环境维护记录包括了维护日期、维护护人、维护设备、故障原因、维护结果等方面内容	符合情况：1指定单位XXXX定期检查感知节点设备、网关节点设备部署环境，记录设备工作状况，并定期维护。2.由外包人员定期检查，提供有外包人员的资质、身份、证明信息。 部分符合情况：由外包人员定期检查维护，未提供有外包人员的资质、身份、证明信息。 不符合情况：未指定专门人员定期对设备部署环境进行检查。

感知节点管理	b)应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确的规定，并进行全程管理	物联网的感知节点往往是大规模部署，并且存在大量无人值守设备，需要对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确的规定，并进行全程管理	核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面	1)感知节点和网关节点设备安全管理文档覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面内容 2)对于远程维护设备的，应具有远程维护安全规范 3)感知节点和网关节点设备安全管理文档，应明确感知节点和网关节点设备到期废弃后，需要对原来采集的数据、访问日志等信息进行及时的备份或销毁管理，部分设备在复用之前需要进行必要的初始化状态重置、缓存数据清理等操作，避免原系统信息的泄露。高敏感数据的存储介质采取物理销毁的方式进行销毁	符合情况：制定有相关的设备管理制度，对感知节点设备、网关节点设备进行管理规范，如入库、存储、部署、维修、报废等，并保留有相关的管理记录。 部分符合情况：制定有相关的设备管理制度，对感知节点设备、网关节点设备进行管理规范，如入库、存储、部署、维修、报废等，无相关记录。 不符合情况：未制定相关的管理制度，也未对感知节点设备、网关节点设备进行规范管理。
	c)应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	物联网的感知节点和网关节点往往包含隐私数据，一旦隐私数据被非法获取，会造成隐私泄漏和恶意跟踪，给用户带来安全隐患。需要加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	1)核查感知节点设备、网关节点设备部署环境的管理文档中是否包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等内容 2)核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录	1)感知节点设备、网关节点设备部署环境的管理文档中包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等内容 2)具有感知节点设备、网关节点设备部署环境的相关保密性管理记录	符合情况：感知节点设备、网关节点设备部署在XXX中，设备部署环境的管理文档中包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等内容，具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。 部分符合情况：无 不符合情况：感知节点设备和网关节点设备部署环境不够隐蔽，未采取措施对设备部署环境进行保密性管理。

第四级增加或增强要求	应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令	可控性是物联网最为特殊的地方，要采取措施来保证物联网不会因为错误而带来控制方面的灾难，包括控制判断的冗余性、控制命令传输渠道的可生存性、控制结果的风险评估能力等。需要对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令，	核查是否能够智能处理不同数据之间的依赖关系和制约关系	物联网设备、服务或者系统对对信息和数据的及时性、安全和隐私保护等方面有特定要求的应用场景(如健康服务、监测系统和紧急服务等)，能够从感知终端、存储的历史背景信息或设定的输入等获取到不同数据之间的依赖关系和制约关系等，并根据这些关系进行智能处理，一类数据达到某个门限时可以影响对另一类数据采集终端的影响	符合情况：通过XXX智能处理不同数据之间的依赖关系和制约关系。 部分符合情况：无 不符合情况：无相关措施或智能处理系统对数据进行分析处理。