白皮书

# 物理访问控制的数字化与网络安全

## 解锁系统和协议的新用途，让企业深度发掘访问控制的潜力，共筑高度智能、更安全的世界

八月 2021

AXIS COMMUNICATIONS

# 目录


**1 概述** 3

**2 简介：访问控制的未来** 3

**3 访问控制市场不断发展并面临挑战** 4

3.1 网络安全凭证（网络成熟度） 4

3.2 安防系统架构的未来 4

3.3 IP与传统访问控制 5

3.4 开放式协议 5

**4 实际应用中的技术壁垒** 5

4.1 RS–485控制器 6

4.2 拥有MAC地址的设备的价值所在 6

**5 良好实践的特质** 6

5.1 利益相关者管理与综合型安防策略 7

5.2 合作伙伴、供货商和供应商的积极参与 7

5.3 安全管理：外部监管与供应商流程 7

**6 指南与工具（供应商流程）** 8

6.1 制造强化配置指南 8

6.2 设备管理 9

6.3 与OEM/ODM相关的挑战 9

6.4 CPU微处理器芯片 9

6.5 固件策略 9

6.6 漏洞管理 10

6.7 安全咨询通知 (Security Advisory Notifications) 10

6.8 构建安全成熟度模型 (BSIMM) 10

6.9 长期支持 (LTS) 10

6.10 学习与合作 11

**7 打造安全的网络环境：未来规划与注意事项** 11

7.1 供应商 11

7.2 产品与系统 12

# 1 概述

云连接的发展正在改变物理安防行业的面貌，迫使安装商顺应行业发展趋势。门禁系统的控制似乎正朝着跨国科技公司的领域发展，随着系统的智能化水平、扩展能力和前端依赖程度日渐攀升，系统本身的价值期待进一步提升。

这样的发展趋势，加之其与企业内其他系统的集成潜力，也意味着网络安全需要在系统开发和部署阶段中，尤其是在依托现有基础设施的场合中，扮演更为重要的角色。在向满足当今和未来需求的数字化访问控制系统转型的进程中，克服串行架构、无MAC地址等技术壁垒是关键的一环。

部署和保护数字化访问控制系统也意味着，要遵守良好的实践方法，保证达到更高的安全水平。我们需要评估和测试系统中所涉及的诸多要素，包括设备、供应商或协议等，这些要素全都需要具备可靠性和稳定性。我们还需要不断掌握威胁状况，并了解如何降低因新发现的漏洞和缺陷所致的风险。

由于供应商的设备要进入企业网络，因此还应尤其注重供应商评审。严谨的供应商应就自己产品制定并发布相应的安全保护流程，具体措施包括：发布强化配置指南、提供专门的管理工具来简化对网络设备的管理和保护，等等。此外，建议供应商还应对自己管理已知漏洞和缺陷的策略持公开和诚实的态度。

# 2 简介：访问控制的未来

云连接为物理安防行业打开了系统部署和利用的新视野。最终用户和买家需要高度智能且更着眼于业务的综合型解决方案，并要求这些解决方案中集成远超传统技术的监控和访问控制能力。

许多供应商基于自己的专业知识、服务以及对物理安防的了解，建立了有效的商业模式。但网络连接能力和物联网 (IoT) 不断改变着行业格局，这就要求物理安防产品的传统供货商和安装商了解开放式平台的IT语言、IP连接和软件集成，以便适应市场变化，保持市场竞争力。

当下，主导权似乎正快速地从电子门禁系统供应商向跨国科技公司转移，后者现在有能力以挑战传统运营方式、重塑安防行业。智能楼宇和智慧城市孕育着巨大的机遇，鉴于当今技术的部署便易性和先进性为智能环境带来了诸多优势，许多人都预测，现代化访问控制市场将出现快速增长。

毫无疑问，托管型访问控制的助推因素是，科技巨头证实了云技术的成功；而在全球新冠疫情期间，对这些技术的依赖则表现得尤为突出。这样的巨头有足够的远见、规模和想象力来推动巨变，众多其他企业在认识到云技术的价值后，也纷纷转向以托管型解决方案来满足自身的安防和商业需求，在这样的形势下，物理安防也将发生变革。

然而，在当下，许多制造商并未就这种不断变化的市场做好准备，依然沿循着以死板的专有设计为基础的商业模式。朝着智能物理安防解决方案的转型与这种传统模式形成了鲜明的对比，而后者则可能受到强有力的挑战。虽然变革不会突如其来，新型云托管解决方案也尚未成为主流，但这样的光明新世界正是现在新入行的工程师们的奋斗目标。

因此，访问控制以及物理安防的未来总体上将取决于对更大价值的预期。访问控制系统将成为数据收集点，门禁控制器将成为智能I/O设备。用于访客管理的二维码以及用于无障碍访问控制的人脸识别技术将越来越多地作为分析功能嵌入在摄像机或传感器中，实现前端管理。对于那些已做好相关准备并助力重塑行业的人来说，访问控制的未来令人兴奋又充满挑战；同时也意味着能够把握切实的机遇，通过创新打造高度智能、更安全的世界。

在本白皮书中，我们介绍了与访问控制尤为相关的方面，其中包括这些系统的许多基本特征。同时，我们还将分析供应商在具体实施时的注意事项，为最终用户提供相关说明和建议，助其以更强的信心与产品和服务提供商展开磋商，制定更明智的采购决策。

# 3 访问控制市场不断发展并面临挑战

在物理访问控制系统 (PACS) 方面，我们往往处理的是与放行与否相关的风险因素。我们需要以平衡的方式设计物理访问控制系统，而这则建立在对潜在威胁的评估基础之上。

现今，场所保护越来越多地采用日益先进的电子访问控制解决方案，这些系统能够快速高效地管理整个企业范围内的门禁，在必要时保留数字足迹以供核查和监控，并与HR和访客管理等其他系统高度整合。

这样的系统整合可提供强大的信息储备，助力商业和安防决策制定，因此，全面评估系统的网络成熟度就变得非常重要。犯罪分子正变得日益狡猾，网络威胁日益加剧，随之而来的挑战在于，要如何消减访问凭证遭到克隆的风险、内部威胁或远程发起的网络攻击。

此外，架构本身也存在问题。许多传统访问控制系统都采用的是过时的基础设施。由于综合型安防技术也通常采用这种基础设施，因此供货商所面临的挑战一方面在于，调整自家的硬件，以便能够连接到这些企业网络，另一方面则在于，认识到IT安全的重要性以及不断变化的安全形势，从而全面评估并防范企业所面临的众多风险。

网络安全方面的考量应成为新安防系统开发过程中的一个关键因素。访问控制技术在物理安防解决方案中扮演着重要的角色，因此在制造时，应遵守公认的网络安全原则、事件报告和实施规范。必须认识到，系统的完整性取决于其薄弱环节。**未准备好迎接风险的系统**即是潜在的风险突破口。如果无法证明系统已准备好迎接风险，并就事件通知和公认的恢复措施制定适当政策，系统就可能无法提供预期的必要物理安全级别。

## 3.1 网络安全凭证（网络成熟度）

IT行业参与度的日渐提升开始改变着技术的评估、部署和维护方式。IT从业人员的一大关键任务是，评估企业的网络安全凭证，重点着眼于供应商的网络安全知识。这也被称为网络成熟度。网络成熟意味着能够对威胁概况和降低风险都有较深入的了解。网络摄像机现有的众多网络安全文档和指南也可以适用于物理访问控制，因为网络风险的挑战、评估和说明以及攻击的潜在破坏力对于这两种产品来说都是差不多的。

## 3.2 安防系统架构的未来

先进的访问控制设备通过网络电缆和RJ45接口实现连接。网络为访问控制器赋能，并助力设备与中央管理系统之间的通信。访问控制行业的推动力是向TCP/IP系统的转型。2013年面市了一款真正支持IP的门禁控制器 (AXIS A1001)，自此，PACS不断发展，现已囊括了丰富的先进功能，而仅靠传统技术，几乎无法达到这样的水平。

这样的创新还有许多，例如，用于简化非接触式访问控制的二维码读取器、通过与网络摄像机集成而实现的脸部识别、以及牌照读取，这些功能通过与PACS数据库交互，能够在前端决定是否放行。IP系统的主要优点包括：安装成本低、配置和设备管理简单。与其他设备的轻松集成意味着，解决方案拥有前瞻性，能够以简单的即插即用式连接兼容新推出的安防技术和增强功能。

### 3.3 IP与传统访问控制

IP系统的优点通过先进的新型访问控制设计得以实现（尤其是最终用户希望标配的非接触式系统）。用户还希望访问控制能够与智能手机和平板电脑的使用相结合，而不仅局限于使用移动式凭证。行业要如何才能提供更好、更有用且更节省时间/成本的访问控制系统，以及这样的系统能否跟得上大型科技企业所推动的创新进程？这些都是行业的供应商侧所面临的挑战。

迄今，这方面的机遇尚未得到利用，其原因可能在于，传统的访问控制系统依赖于安装在串行架构中的门禁控制器，并通过RS-485电缆连接到中央设备或服务器。而且，大多数系统还是专有系统，这就意味着，门禁控制器被“锁定”，只能通过供应商指定的软件进行管理。这就将最终用户绑定到单一的软硬件供应商，而这些系统往往较为复杂，从而需要专业人员来完成安装和配置。

在扩展传统的门禁系统时，过程也较为繁杂，因为中央控制器通常被设计成兼容特定数量的门禁，由于系统灵活性有限，如要部署非标准型配置，便需要投入高成本。例如，仅仅是增加一道门禁，成本便可能大大提高，这就使扩展变得过于昂贵。

IP网络允许纳入更简洁且易于安装的PACS架构，灵活性和定制性大大提升。IT从业人员对真IP设备及其在联网型访问控制系统中的应用有着强烈的偏好。在未来的设计过程中吸纳这样的人才有着重要意义，他们将保证这些IP设备得到合理利用，这也将大大有助于降低扩展成本，并将成为未来访问控制设计的一大要求。

### 3.4 开放式协议

访问控制的未来与制造商在开放式协议环境中分享自身技能和能力的意愿息息相关。对这种开放持拒绝态度的大有人在，许多门禁系统开发企业似乎都倾向于将最终用户绑定到自己的解决方案上，以保证未来的收入。但这种措施几乎没有长期价值。用户对解决方案的要求越来越高，为此，也非常愿意分享自己的数据。

系统设计厂商和门禁硬件供应商鲜有足够的资源或IT专业知识来保证为用户提供用于建构综合型物理安防系统的众多解决方案。许多厂商甚至似乎没有意识到，面对新的创新型解决方案，自己的产品和服务正快速变得黯然失色，而且这些创新型解决方案不仅威胁着他们的商业模式，而且还威胁着他们在访问控制市场上的地位。这就是高新技术系统的能力，同时也是现代创新的速度，它们让市场对门禁控制器的需求日渐降低，并代之以智能I/O设备。

开放让供货商能够提供适用于小型门禁系统的设备，实现简洁部署与采购安装成本的双效收益。在后期，还可以视需要对这些设备进行调整，以适应更大规模、技术上更复杂的运营。这种灵活性是现代安防的特质，保障了现下所购买的系统仍能够满足未来需求，契合用户的商业增长和需求变化。

有关开放环境和开放技术的更多详情，请访问ONVIF网站*www.onvif.org*，ONVIF是一个行业机构，旨在推动开放式标准的开发。

## 4 实际应用中的技术壁垒

在实现数字化访问控制的技术连接、接口和设备方面，有许多要考虑的因素。在从传统系统向支持云的系统迁移的过程中，可能涉及许多方面。下文将详细介绍在利用现有技术时必须注意的方面、以及与之相关的流程，以免在升级和应用新解决方案时遭遇壁垒。

### 4.1 RS–485控制器

RS–485控制器的部署以及安装半智能设备的潜在风险是一大考虑要素（这些半智能设备基本上没有介质访问控制 (MAC) 地址，难以识别）。RS–485又称为TIA–485(–A) 或EIA–485，是定义串行通信系统中驱动器和接收器的电气特性的标准。电信号可被均衡，也可以支持多点系统。但RS–485仅指定物理层，即，发生器和接收器。它不管控重要的通信层。

请注意，无MAC地址或者采用串行架构本身并不对访问控制系统的运行造成可靠性问题或有害影响：这样的设计在30多年以来，一直是访问控制的支柱。然而，除非访问控制系统中的控制设备都是智能设备且能够单独寻址，否则便难以显著提升安防水平。这里的基本条件是，只有高度智能化的系统和完全可访问的设备才能够提供预期的未来价值。请注意，“完全可访问”并不意味着网络安全水平欠佳的设备，而是与这截然相反。

#### 4.1.1 开放式监控设备协议 (OSDP)

IEC所采用的能够提高访问通信安全的新通信方法是开放式监控设备协议 (OSDP)；它是一种访问控制通信标准，由安防行业协会 (SIA) 制定，旨在改善访问控制和安防产品间的互操作性。OSDP采用128位加密，支持多点安装，能够监控连接并相应地报告读取器问题。还需指出的是，OSDP支持读卡器、电子门锁、报警触点、以及2线制开门功能（不同于以往每道门所需的复杂接线）。SIA网站报告指出：“OSDP已于2020年被国际电工技术协会认定为一项国际标准，并将于2020年7月编为IEC 60839–11–5正式出版。为保持行业低位，SIA OSDP将不断优化。”

### 4.2 拥有MAC地址的设备的价值所在

MAC是个体网络适配器或设备的全局唯一硬件地址。在IT联网中，MAC地址的每个位都非常重要，它们都是IP地址的组成部分。MAC地址唯一性地标识LAN上的计算机，是TCP/IP等网络协议发挥用途的必备要素。MAC地址被硬编码到设备中，它能够通过操作系统进行模仿，但是当然不建议这么做，这个地址应受到安全解决方案的保护。

TCP/IP和其他主流网络架构通常采用开放系统互连 (OSI) 模型，其中，网络功能被划分为多层。MAC地址功能处于数据链路层（OSI模型中的第2层），它们让计算机能够实现在网络上的唯一标识。MAC地址过滤进一步增强了安全。在允许设备联网之前，路由器对照认可地址列表，检查设备的MAC地址。如果客户端地址在路由器的这个列表中在列，则对此地址放行，否则，便会拒绝此地址。

#### 4.2.1 以太网供电（PoE）

PoE在其应用中发挥着两大优势：节省成本、以及灵活的设备安装。PoE以同一条电缆负责数据和电力输送任务这就意味着，相较于传统设计，设备架构得以简化。需要指出的是，支持IP连接是许多访问控制系统的一大卖点。

## 5 良好实践的特质

访问控制管理是有效应对人流和控制门禁的重要环节。企业需要的远不仅限于锁门或布设路障，而是以更好的控制方案来持续保障更好的客户服务关系和更高的安全水平。综合访问控制中的良好实践不只是选择合适的工具，而是涉及组建合适的架构；采用优质技术；遵守相应的规程和协议；鼓励员工和利益相关者秉持正确的态度、采取正确的行为。

## 5.1 利益相关者管理与综合型安防策略

我们可以看到，同一基础设施中通常集成了多种技术，以便以所需的运营技术保障这些场所的顺畅运行，因此，我们也需要制定综合的决策制定流程。综合型安防措施突破传统束缚、助力不同商业团队共同协作的成功案例并不鲜见。在当今，传统的电子和物理安防设施与企业网络并驾齐驱，因此，这样的综合已变得尤为重要。

必须注意的是，安保团队能够依赖辅助其工作需求并应对相关风险的技术，同时，还必须助推IT安防策略并使物理设备不变成公司网络的后门。通过利益相关者的共同协作，能够打造安全的网络和物理环境。

## 5.2 合作伙伴、供货商和供应商的积极参与

务必让第三方理解“一切以安全为前提”的重要性，以及第三方的运营是在此基础上进行并符合具体需求的。与第三方的关系是建立健康供应链、铸就强力互信纽带的关键。

在评估第三方及其对供应链的影响时，有以下几个关键方面：

- 他们了解并承认相关的网络安全风险
- 他们能够证明在现有流程和工具中纳入了成熟的网络安全措施
- 他们了解法律法规对其业务的影响
- 他们能够证明自己将如何帮助用户达到合规要求
- 网络安全是一个过程，而不仅仅是技术——他们能够证明自己的网络安全寿命期管理对用户企业的保护力。

## 5.3 安全管理：外部监管与供应商流程

与大多数有效的安全防护类似，网络安全也关系到防御深度。其中涉及为IP摄像机网络提供适当保护；从产品和合作伙伴选择，到要求设定。

### 5.3.1 标准与指令

ISO/IEC 27001——信息安全管理；ISO/IEC 27001为安全管理体系，其中要求：

- 对企业的信息安全风险进行系统性评估，其中要考虑相关威胁、隐患和影响
- 设计并部署相辅相成、覆盖面广的信息安全控制和/或其他风险处理（如风险规避或风险转移）措施，应对那些被认定为不可接受的风险
- 采用综合管理流程，保障信息安全控制持续满足企业的信息安全需求。

### 5.3.2 Cyber Essentials Plus

Cyber Essentials是一个以政府为后盾、由行业支持的计划，旨在帮助企业保护自身免遭常见网上威胁的侵害。Cyber Essentials能够有效指示企业对网络安全挑战的理解程度，并评估公司的策略和流程。具体评估方面包括：

- 安全配置
- 访问控制和管理

- 恶意软件防护
- 补丁管理
- 防火墙和互联网网关

对于技术开发商来说，第一道防线应该是消减与自家系统相关的风险。从2014年10月1日起，政府要求，涉及处理特定敏感信息和个人信息的项目的投标供应商都必须获得Cyber Essentials计划的认证。

### 5.3.3 设计安全、默认安全

**设计安全、默认安全**由监控摄像机理事会于2019年施行，对监控摄像机系统和组件的制造商设定了基本要求。它要求制造商以整体性途径从根本上解决安全问题，而不是仅处理问题表象；以规模化的方式降低对系统或特定类型的组件造成的总体危害。

“设计安全、默认安全”要求在技术上做长期努力，保证为软硬件配备适当的安全保护。它还涉及一项同样艰巨的任务，即，保证这些保护措施能够在市面上轻松获得，并能够发挥相应效用。

为了给技术提供支撑，安讯士在以下方面将“设计安全、默认安全”与“国家网络安全策略”行为规范相统一：

- 密码提示
- 密码强度指示
- HTTPS加密
- 802.1x
- 禁用远程访问（NAT穿越）

# 6 指南与工具（供应商流程）

就网络保护而言，企业通常要部署多项技术控制措施，打造“多层防御”体系，以便限制个体故障点和暴露点的数量。然而，通常被忽略的一个重要过程便是“系统强化”，它涉及更改默认系统设置，这样，就能够进一步提升系统在面对信息安全威胁时的安全性。此外，这个过程还有助于减少系统内部的固有隐患。

## 6.1 制造强化配置指南

系统强化过程应落实到联网设备，其中包括工作站、服务器和其他网络设备。制造商对其系统设置和配置的了解优于他人，因此应负责向合作伙伴和用户提供必要信息，以帮助他们保护设备和最终用户资产的完整性。强化配置指南应为参与视频监控解决方案部署的人员提供技术建议。它不仅应明确基准配置，还应就应对日益猖獗的网络威胁，提供丰富的信息参考。

供应商在设备的设计、开发和测试过程中应运用网络安全实践，以期更大程度减少可能被网络攻击利用的漏洞。然而，保护网络及其设备以及网络所支持的服务需要整个供应商供应链以及最终用户企业的积极参与。安全的环境取决于其用户、进程和技术。合理的强化配置指南应遵守基准应用规范，如“CIS控制”第6.1版。这些控制先前被称为“SANS 20个关键安全控制”(SANS Top 20 Critical Security Controls)。

## 6.2 设备管理

设备管理器是一种预置工具，可提供一种简单、经济合算且安全的方式来管理互连设备。它为安装人员和系统管理员提供了管理重要安装、安全和维护任务的高效工具。

设备目录/资产管理系统：

- 帐户和密码策略
- 高效安装固件升级和应用程序
- 应用网络安全控件——管理HTTPS以及上传IEEE 802.1x证书、管理帐号和密码
- 证书生命周期管理——管理重要安装、安全和运行任务
- 快速、便捷配置新设备——备份和恢复设置
- 适用于不同规模的场所——单点或多点安装

## 6.3 与OEM/ODM相关的挑战

原始设备制造商 (OEM) 是指以自己的名称和品牌转售其他公司的产品的制造商。原始设计制造商 (ODM) 是指按照其他公司指定的规格设计和制造产品的公司，所述产品最终由该其他公司以其自己的品牌进行销售。这样的制造商让品牌公司能够在不必建立或运行工厂的情况下实现生产。

制造商通过OEM或ODM获得来自其他供应商的产品有着许多优势。首先是，消除了制造风险和成本，让企业能够集中精力开展销售和市场营销事宜。这是安防行业许多摄像机制造商以OEM或ODM形式生产贴牌产品的主要原因之一。

这样的经营方式会带来若干问题，其中较明显的问题便是网络安全。如果其中一家制造商存在隐患，就可能影响到整个供应链上的其他分销商及合作伙伴。它还可能大大降低供应链的透明度。由于运营中涉及的OEM和ODM数量较多，开展尽职调查并拒绝使用特定制造商的技术的最终用户可能最后在不经意间变相用到这些技术，而自己却浑然不觉。

## 6.4 CPU微处理器芯片

已经显而易见的是，安装到设备中的一般CPU处理芯片有着较多隐患，正成为黑客的攻击目标。其中一个主要原因在于，攻击可以通过一个已知漏洞蔓延开来。Meltdown和Spectre漏洞攻击就是发生在近期的此类案例，这是两种相关的单通道攻击，针对先进的CPU微处理器，能够利用未授权的代码非法访问数据。

大多数设备（从智能手机到数据中心的硬件）都可能存在一定程度的隐患。主流操作系统供应商制作了补丁来解决这样的问题，但某些补丁包含平台特有的元素，需要由设备制造商 (OEM) 安装。国家网络安全中心 (NCSC) 建议尽早为设备打补丁。

## 6.5 固件策略

签名固件对于最终用户有着重要意义，它能够在一定程度上降低设备在物流和/或配送流程中遭到篡改的潜在风险。签名有时又称为哈希，在固件发行时附加到固件。处理器将计算自己的哈希，只有在固件映像的哈希与处理器信任的证书所签名的哈希匹配时，才会加载固件映像。

## 6.6 漏洞管理

网络犯罪及其相关风险的持续攀升促使许多企业提高了对信息安全的关注度。漏洞管理流程应成为企业管控信息安全风险的要务之一。这个流程将允许企业持续总览其IT环境中的漏洞以及与这些漏洞相关的风险。只有发现并消除IT环境中的漏洞，才能够防止攻击者入侵企业网络并窃取信息。

供应商务必要将漏洞管理纳入自己的运营活动中，这样的漏洞管理包括检测和修复系统漏洞、以及防止在更改过程和新系统部署过程中产生新漏洞。如果是与供应商接受的风险相关的问题，应告知最终用户，并应获得最终用户的认可。如不遵守这一原则，攻击者可能利用系统内的漏洞对企业及其供应商发起网络攻击。

必须按照经认可的流程及时安装IT安全补丁和安全漏洞更新，以免遭到入侵破坏。如果出于某种原因，无法更新供应商系统，则必须采取措施保护脆弱的系统。进行更改时，必须遵守供应商的更改管理流程。

## 6.7 安全咨询通知 (Security Advisory Notifications)

安全咨询有助于降低因已知漏洞所致的风险。安全咨询可以涉及官方CVE（通用漏洞披露）或其他漏洞报告，它可以包括漏洞描述、风险评估、措施建议、以及与服务发行时间有关的信息。大多数供应商都部署了间接销售模型，并制定了合作伙伴计划。

安全咨询通知 (Security Advisory Notifications) 让未加入制造商合作伙伴计划的客户能够尽早以及在向公告渠道发出公告时，获得相关的网络安全通知。对于安装了设备但却未与最初实施安装的公司订立合同的最终用户，安全咨询通知是一个非常重要的工具。

## 6.8 构建安全成熟度模型 (BSIMM)

BSIMM是一种软件安全评估框架，用于帮助企业将自己的软件安全与其他企业的措施进行比较，明确自己的位置所在。BSIMM有助于评估流程、活动、角色和责任，具体体现在以下方面：

- 进行设计和架构评审
- 进行标准规范审查
- 测试已知漏洞
- 运行标准漏洞扫描工具，查找开放式源代码包中的CVE漏洞

## 6.9 长期支持 (LTS)

长期支持 (LTS) 是一种产品寿命期管理策略，即，在标准版本发行后的较长时间内，持续稳定发行相关软件。“长期支持”固件只应包含用于保障稳定性、性能和安全性的补丁。自设备面市之日起，供应商应在长达10年的时间内提供LTS固件。

LTS应与现有软件支持并行，但应独立于现有软件支持。LTS支持的一大优点在于，它有助于与原始固件版本相关的第三方保持协调一致。

### 6.10学习与合作

选择技术供应商时，一个重要的考虑因素是培训以及可用的支持服务。随着供应链渠道和行业面临的挑战增大，尤其是网络安全方面的挑战增大，制造商应着眼于前瞻性地解决相关问题，为市场提供可靠且满足需求的产品和服务。可能的例子包括：

- 以网络安全为主题的课堂形式免费课程
- 网络安全在线培训
- 网络安全在线快速检测
- 强化配置指南
- 漏洞修复策略
- 良好的网络安全实践
- 网络安全概念与术语

# 7 打造安全的网络环境：未来规划与注意事项

良好的网络安全涉及识别企业关键服务和产品所面临的风险、确定这些风险的优先级以及对风险做出响应。落实良好的网络健康安全实践将有助于防止数据外泄和不正确的系统配置，同时尽可能降低企业的相关风险。利益相关者也必须就关键威胁领域达成一致，着眼于风险管理的主要目标。

下面的注意事项虽未详尽列出，但将有助于提升面对网络威胁时的处理效率。

## 7.1 供应商

**检查注册信息和认证证书**

核查相应的注册信息和认证证书：比如，要求查看ISO9000注册信息以及其他质量认证证书。判定供应商的产品设计是否适用于企业网络。

**检查是否遵守良好实践**

保证所选择的供应商能够证明其良好的网络安全实践。供应商应提供网络强化配置指南，其中需描述网络和物理安全措施以及有助于保护网络的良好实践。

**审查供应商**

在决定购买之前，开展较全面的审查。检查供应商的商业条款，保证这些条目是清晰透明的。从财务角度讲，必须弄清楚在遇到经营问题时，产品和支持服务会受到什么样的影响。

**明确相关资源，保障后续支持**

判断供应商是否拥有相应的资源，以便持续打造符合您未来需求的解决方案。判断供应商的规模、业务范围和能力是否能够支撑您持续增长的商业需求。

**明确未来商业需求**

关注您的未来需求。智能设备和解决方案拥有增强和长效保障商业发展的潜力，因此供应商应能够以合适的维护协议和持续支持满足或超越您的预期。

### 检查商业实践是否与伦理道德相符

检查企业实践是否符合伦理道德且具有可持续性。建立在互信与共同目标基础上的合作关系能够为长效合作奠定坚实的基础。供应商是否制定了恰当的环境管理体系、企业社会责任 (CSR) 计划或符合伦理的采购政策?

## 7.2 产品与系统

### 开展尽职调查

对系统及其核心构件开展技术层面的尽职调查，保证符合预期并且不存在可能影响持续运行的隐患。切实就风险评估和风险降低提供了清晰的说明。

### 检查维护合同

检查合同内容，比如，服务和维护合同是否涵盖了制造商软件更新和固件升级。

### 保护联网设备

保证联网的物理安防系统是安全的。安防系统的部署应兼顾网络安全；应修改默认用户名和密码；应安装新版固件；应采用了加密（优选HTTPS加密）；应禁用远程访问。

### 要求提供设计安全声明

供应商应能够提供设计安全声明，以证明其联网设备的网络安全状态。

### 打造智能化系统

高度智能的联网设备指使用MAC地址联网的那些设备，它们构成系统架构的内在组成部分。无MAC地址的设备不是智能设备，无法被单独识别、管理或保护。

### 评估是否符合GDPR/数据保护法案

GDPR于2018年正式施行，同年还施行了“1998年数据保护法案”的更新版本。保证产品和系统能够符合“2018年数据保护法案”和GDPR。

T10168631/zh/M3.2/2108

# 关于 Axis Communications

Axis 通过打造解决方案，不断提供改善 以提高安全性和业务绩效。 作为网络技术 公司和行业领导者，Axis 提供视频监控解决方案， 访问控制、对讲以及音频系统的相关产品和服务。 并通过 智能分析应用实现增强，通过高品质培训提供支持。

Axis 在 50 多个国家/地区拥有约 4,000 名敬业的员工 并与全球的技术和系统集成合作伙伴合作 为客户带来解决方案。 Axis 成立于 1984 年，总部 在瑞典隆德