

智能监控保护机场周界安全

研究传感器选项、应用软件和关键影响因素，确保为众多行业提供具有前瞻性的安防解决方案

七月 2021

目录

1	概述	3
2	引言	3
3	周界保护解决方案	4
	3.1 物理解决方案	4
	3.2 物理周界的入侵侦测	4
	3.3 其他入侵侦测传感器	4
4	基于视频的解决方案	4
	4.1 视频摄像机的应用	4
	4.2 热图视频监控解决方案	5
	4.3 可见光摄像机	5
	4.4 视频内容分析	5
5	成本	6
	5.1 评估并衡量投资回报	6
	5.2 成本评估	7
6	安讯士公司的提议	7

1 概述

围栏通常是场所安防监控的“外保护层”的基本组成部分，它可以是屏障、围网或威慑物的形式，将人和动物都阻挡在外。由于物理屏障仅能够拖延或妨碍入侵，因此可以加入其他设施来增强围栏的威力。

可沿围栏部署多种类型的侦测装置。基于电缆的侦测器能够沿围栏布设，而在具有战略意义的位置，则可以放置雷达（微波）传感器、红外光栅或激光器。

受动物、晃动的植物和树、恶劣天气等因素的影响，这些类型的侦测装置都可能产生假警报。此外，还可能存在其他影响因素，例如，使用微波传感器时的频率冲突、或者安装环境的物理限制。

对于希望监控大型场所或多个场所的客户而言，摄像机的优点显而易见。先进的网络视频解决方案能够将摄像机内的运算处理与人工智能相结合。这项技术所固有的可扩展性、有效性和威慑性意味着，视频摄像机是安防系统的一种高性价比的补充。

虽然摄像机和移动侦测软件扩展了周界保护的范围和能力，但这些解决方案可能因无法在恶劣天气条件下可靠侦测而应用有限。在经过适当校准且搭载有视频分析工具的情况下，热成像摄像机能够提供有效的监控和监视，不受光线条件影响，几乎无惧恶劣天气。

一段时间以来，视频分析取得了显著的成就，现已得到广泛应用，甚至在面向家用安防市场的摄像机中，也配备有此功能。在使用了分析工具的情况下，仅会录制包含相关活动的视频，从而能够降低对存储空间的需求。通过网络摄像机本身中处理大部分录像，网络上的负载会大幅下降，因为只对相关的摄像机视频进行流处理。这在控制室场景中有着突出的优势。

与其他安防措施一样，周界保护解决方案的评估应兼具适宜性和恰当性。首要目标一如既往是应对威胁。

融合安防方法正在迅速成为更佳的做法，它结合了来自IT和运营等其他部门的意见和考量。这包括需要尽早地让这些处理工程的人员参与进来。

众所周知，要证明用于防范意外事件的安防解决方案的投资回报率，通常较为困难。这主要是因为它不产生潜在收入，无法对比成本加以衡量。证明更为切实的ROI是可行的；例如：解决方案不仅向人员发出警报，告知可疑行为或入侵，而且还可以执行自动响应。

2 引言

电子周界保护解决方案一直以来都深受高度重视安全性的政府和商业场所或富豪的青睐。在技术进步、市场竞争日益激烈并由此推动成本降低的形势下，技术含量相对较高的解决方案现在有着更广泛的应用空间。

那么，现代化周界保护解决方案都包含哪些组成部分呢？技术在工作中扮演着怎样的角色，以及它是如何提供安全保障和切实保护的？

本白皮书将介绍当前用于周界保护的一些基于传感器的选项，并对解决方案背后的技术支持加以分析。

3 周界保护解决方案

3.1 物理解决方案

物理解决方案通常是场所分区域监控的“外保护层”的基本组成部分，一般情况下由周界围栏构成，通常用铁丝网或焊接网、焊接板或混凝土板材搭建。周界围栏有许多用途，其中一个主要用途是，提供能够拖延或阻止入侵的物理屏障。围栏在隔离保护资产的同时，也能防止受到监控；并且它有威慑作用，能够防止动物进入。此外，还可以加入防攀爬装置、规定的车辆出入路线、防越界装置、围网等设施，使周界围栏发挥更强的效力。

然而，物理屏障仅能够拖延入侵。因此，还应为周界配置自动入侵侦测技术，以便能够提供可验证的实时警报、位置数据、目标追踪，并能够打包证据和数据以供事后调查之用。

3.2 物理周界的入侵侦测

通常使用多种类型的电缆式“侦测器”来保障大型周界的安全。这些基于电缆的侦测器通常埋设在地下或安装在围栏上，它们沿围栏布设，并且不需要布置成直线。它们还能够覆盖拐角周围的区域以及**地面盲区**。一些供应商提供的围栏配备自动侦测解决方案。

与其他侦测解决方案一样，基于电缆的侦测器可能产生假警报，也就是“误报警”。造成误报的常见原因有动物、晃动的植物和树、恶劣的天气等。基于电缆的解决方案在视频监控的加持下，可以更好的发挥作用。视频不仅可用于验证入侵，而且还可用于查明报警原因。基于电缆的解决方案仅可针对入侵本身发出警报；它无法提供与入侵者数量等有关的信息，亦无法提供为准备应对而所需的其他细节。

3.3 其他入侵侦测传感器

围绕周界，在具有战略意义的位置部署其他入侵侦测装置，如雷达（微波）传感器、红外警戒线或激光器。这些技术同样有着诸如误报警等问题，而且如果未正确遵守安装要求，在面对特定距离和高度时，它们的侦测能力也较为有限。

在采用了其他电子设备的环境中，周界上的雷达使用可能会非常麻烦。这些设备的工作频率和频谱可能与雷达相同，虽然通过精心选择频率并且限制功率，能够降低干扰，但设备自身的有效工作范围也将受影响。

4 基于视频的解决方案

4.1 视频摄像机的应用

过去的独立式传统CCTV技术与当今市面上的高科技网络摄像机解决方案相去甚远。先进的网络解决方案能够将摄像机内的运算处理与人工智能相结合。然而，这样的技术水平仅在近段时间才达到，且仍处于发展的初始阶段。

对于希望监控大型场所或多个场所的客户而言，摄像机的优点显而易见。这项技术所固有的可扩展性、有效性和威慑性意味着，视频摄像机是安防系统的一种高性价比的补充。

根据当地法律法规，可以依托摄像机技术实现超越物理周界的监视，从而进一步增大监控范围，让操作人员有更多时间来做出响应。采用了视频分析工具的解决方案能够根据预设规则

触发报警。例如，在有人进入距离围栏50米的范围内时，报警触发；如果此人继续在这里徘徊，或者进入距离围栏10米的区域，则可能触发更高级别的报警。

4.2 热图视频监控解决方案

视频监控摄像机与移动侦测软件组合可扩展周界保护解决方案的侦测范围和能力，实现从简单侦测向复杂入侵分析的飞跃。然而，视频的有效性可能因无法在恶劣天气条件下可靠侦测而严重受限。

随着热成像摄像机技术的可用性提高，它们在周界保护上的应用日益广泛。在经过适当校准且搭载有视频分析工具的情况下，热成像（热图）摄像机能够提供有效的监控和监视，不受光线条件影响，几乎无惧恶劣天气。较之于典型可见光摄像机，采用热技术的传感器能够提供卓越的对比度，加之其入侵侦测能力广泛提升，因此非常适合周界保护应用。

热传感器利用车辆或人等目标发出的红外辐射来形成图像。在与视频分析工具相结合的情况下，拥有强大处理能力的先进热成像摄像机能够区分不同类型的入侵目标，并基于一系列预设条件向操作人员发送警报。这些条件可能包括人或车辆的行进方向和速度。传统摄像机也能够做到这一点，但它们需要使用可见光。下一节将详细介绍这些摄像机。

4.3 可见光摄像机

标准可见光监控摄像机需要借助自然光或人造光来提供图像。支持视频监控的光照是一个独立的专业领域，针对这个重要的主题，曾先后发表过多篇文章。但我们仍需要强调一个明显却重要的要点：标准摄像机需要可见光。环境中的光可能构成一大挑战，当光线质量变化时，效果变化也非常明显。尤其是那些负责选定解决方案的人有时会忽略或不明白天气的影响。

热成像摄像机固然有众多优点，但这并不意味着热成像摄像机应该或能够直接取代可见光摄像机——它们还远远没有达到这个级别。这两种技术在集成到同一解决方案中时，可以更好的发挥作用。传统摄像机没有热成像摄像机那样的目标侦测能力；但热成像摄像机也不能像可见光摄像机那样，提供用于取证的细节呈现。这两种技术通常相辅相成，热成像摄像机提供侦测报警，而可见光摄像机的细节优势则保障了证据效力和目标追踪。

4.4 视频内容分析

网络视频监控让安防系统的规模得到空前发展。有效的权限架构能够实现受控的视频访问、分布和存储，期间所涉及的利益相关者数量在理论上不受限制。特别是一项技术进步在扩展能力方面开辟了更高的维度——视频分析。

一段时间以来，视频分析取得了显著成就，这尤其要得益于IP摄像机技术的发展。这在面向家用安防市场的摄像机中可见一斑，许多这样的摄像机现在都集成有一定程度的分析功能，让它们能够（比如）侦测场景中的运动。摄像机还可能“绑定”有某些其他功能，包括越线侦测、运动目标侦测，或者甚至人数统计。

在使用了视频分析工具的情况下，仅会记录包含相关活动的视频，从而能够降低对存储空间的需求。而且，通过网络摄像机本身中处理尽可能多的录像（被称为“前端智能”），网络上的负载会大幅下降，因为只对相关的摄像机视频进行流处理。这在控制室场景中有着突出的优势，安保人员在接到警报时，只需查看视频即可；对于安保人员和企业本身来说，这是工作效率的一大提升。

有两大类系统架构可进行视频分析：集中式和分布式。对于集中式架构，视频和其它信息由摄像机和传感器收集，并传至中央服务器进行分析。在分布式架构中，前端设备（网络摄像机和视频编码器）自身能够处理视频并提取相关信息。前端分析消除了对专用分析服务器的

需求，由于只有在将视频数据传送至中央服务器时，才需要执行压缩，因此现在可以对未压缩的视频内容进行分析。结果是形成了一个更具成本效益和灵活性的架构。事实上，那些曾经因处理能力有限而通常只能处理少量视频流的服务器现在则能够处理成百上千的视频流，因为许多处理工作都已在摄像机中完成。

4.4.1 处理速度与GPU

虽然Gordon E Moore准确预测了处理速度和能力的指数级增长（aka Moore定律），并且一些先进的高科技公司基于此定律预测，在不久的将来，这种增长将放缓，但就当下而言，处理能力得到提升的同时尺寸也在缩小，这表明摄像机制造商和软件开发商能够改变处理能力的利用方式。

截至最近，处理能力的提升大多用于改善图像质量，即，提高分辨率和视频压缩效率。目前来看，市场在图像分辨率提升方面似乎达到了需求峰值。因此，制造商现正利用处理能力来进一步提升前端的智能水平。在很多情况下，这意味着，基于服务器且功能强大的视频分析工具现在能够在摄像机中执行处理。

先进处理器的更小更快的特点让摄像机能够装入图形处理单元 (GPU)，从而提供并行处理能力，开拓新机遇和新的分析可能性。这种新能力让软件开发商将注意力转移到更新前端设备中的现有且经实践验证的服务器分析工具上来，从而推动对更智能的摄像机的需求，能够带来远超安防和视频监控本身的价值。

4.4.2 深度学习与人工智能 (AI)

前端GPU的分析性能实现了飞跃式提升，但监控环境对支持诸如人数统计、占用管理等功能的其他技术类型的需求仍在攀升。得益于AI和机器学习的发展，摄像机中能够集成正展现变革潜力的深度学习处理单元 (DLPU)。

DLPU专为深度学习分析工具的拓展应用而打造。基于深度学习的分析工具能够以卓越的准确度保障侦测和分类，因为其算法能够基于一系列预设目标的表现进行有效训练。这就意味着，周界的入侵侦测解决方案能够被设置为仅针对非常具体的目标和场景发出警报；它是“if-this-then-this” (ITTT) 的高级版本。

在某些情况下，可能只能看到目标的一部分，比如汽车的后保险杠，但系统的分析工具仍能够辨识和识别该车。截止本文撰写之时，尽管有一些其他说法，但市面上的大多数经验证的解决方案都仅限于识别和区分人和车辆类型。然而，能够进行更细致区分（如区分人员身着衣服的颜色）的基于摄像机的分析模型尚处于早期测试阶段。

这种技术进步有可能造就更有针对性的侦测系统，能够识别并区分员工、顾客、公众或潜在威胁。从安防角度讲，通过将先进的分析工具与成熟的物理安防相结合，定然能够打造出效率和准确度更高的犯罪侦测及防范系统。下个阶段的能力提升也许就发生在不久的将来。

5 成本

5.1 评估并衡量投资回报

与其他安防措施一样，从安防漏洞或防御能力角度讲，周界保护解决方案的评估应兼具适宜性和恰当性。首要目标一如既往是应对威胁，对于当今的大多数大型企业或政府场所而言，这些威胁可能是意外闯入者，也可能是抗议者，或者甚至可能是恐怖分子，涉及范围极广。

融合安防方法正在迅速成为更佳的做法，它结合了来自IT和运营等其他部门的意见和考量。这包括需要并且应该尽早地让这些具有工程要求从业经历的人员参与进来。在考虑要采取的措

施时，周界防护历来都采用更为传统的手段，这是一个良好的开端，通常能够制止和拖延潜在入侵者。在这之后，安防设计人员才能继而设计“附连的”技术侦测系统。而现在，众多措施和系统相互集成，因此就需要提早引入更周全、更整体的方案。

众所周知，要证明用于防范意外事件的安防解决方案的投资回报率，通常较为困难。这主要是因为它不产生潜在收入，无法对比成本加以衡量。通常，安保人员需要与财务部门的工作人员协作，才能明确不同类型的安防事件所导致的成本；包括由资产损失/损坏所产生的直接成本，或者更间接但同样会造成声誉损失的相关损坏成本。

然而，证明更为切实的ROI是可行的，这尤其体现在某些技术能够减少特定人工活动或者允许将安保人员调度到其他任务的时候。相应解决方案的例子可能是：解决方案不仅向人员发出警报，告知可疑行为或入侵，而且还可以执行自动“软”响应。这其中可能就包括能够播放预录制播报的IP音频系统，或者通过让标示物亮起，向潜在入侵者告知他们已被侦测到并指示他们离开所在区域。

如果解决方案中加入了监控摄像机，那么可以通过向入侵者显示其某些身份识别证据，例如：使用屏幕显示其车辆牌照或者甚至入侵者自身的图像，从而进一步提高效率。只有在这样的措施无法产生预期效果时，才需要派遣安保团队以开展调查或采取更直接的行动。对警报的这种分阶段应对方法可能更适用于周界外部，但它们确实也有助于降低对安保人员在早期介入的需求，从而解放了人工，带来了明显的收益。

5.2 成本评估

成本估算应基于总体拥有成本 (TCO) 计算。所述TCO包括解决方案在其整个寿命期内的各方面成本：材料和人工成本、研究成本、系统安装成本、运行成本、维护成本、退役和回收成本。这可能需要财务和采购部门更改估算方法，因为资金可能需要在运营与资金费用预算之间重新分配。

与其他有形资产一样，企业需要知道周界侦测解决方案的使用寿命。安防和IT经理可以说明和演示作为未来解决方案的适当技术将如何节省开支，从而为财务部人员的工作提供帮助。先进智能监控设备的特点在于，在一定程度上具有内在前瞻性。也就是说，拥有适当处理能力的设备能够随时间推移反复利用技术发展成果，而这主要通过基于AI和机器学习的处理分析工具来实现。

6 安讯士公司的提议

安讯士为集成合作伙伴的解决方案提供了开放式途径，这就意味着，在与可靠的视频分析工具相结合的情况下，其联网的传感器让客户能够部署高性能集成式周界保护解决方案，这些方案兼顾了整个企业以及整个系统寿命期内的网络安全和成本效益。

在不适用热传感器的地方，微波技术（雷达）是不错的替代选择，它有着许多与热技术相同的优点，并能够潜在地减少误报警。与较先进的监控摄像机一样，安讯士雷达技术也可受益于机器学习和深度学习。安讯士雷达装置能够准确侦测、分类和追踪人和车辆，误报率接近零。

雷达技术支持24/7不间断运行，几乎不受晃动的阴影或光束、小动物或昆虫、恶劣天气条件等常见假警报触发原因的影响。这就能够实现成本效益高的运行，确保安保人员能够集中精力应对已确认的真正威胁。雷达还能够提供目标速度信息，从而实现对接触点的准确计算，或者甚至强制限速。

解决方案的性能通常是信息请求 (RFI) 或市场分析调查问卷的首要组成部分。安讯士摄像机搭载安讯士自研的ARTPEC处理器，其处理能力备受业界好评，让您能够在摄像机中（前端）嵌

入某些先进的周界保护视频分析解决方案。重要的是，解决方案采用的是安讯士自研的技术，而非第三方组件，令您使用更安心。

这种“前端”智能意味着，多台摄像机因此能够同时追踪发生在不同场所的多个事件。这种分布式技术架构让您能够扩展解决方案，根据需要增加摄像机数量，同时无需投资购入集中式服务器技术。

AXIS Perimeter Defender (APD) 通过了英国政府认证，能够侦测四种不同类型的事件，查找一个或多个具体的人或车辆：

- 入侵预定义区域
- 以预定的顺序和方向通过区域
- 在一定条件下通过区域
- 有无徘徊逗留人员

APD的功能并不仅限于入侵报警和相应的视频显示。它还能够提供可叠加到视频上显示的元数据，进而显示边界以及人员和车辆的活动轨迹。在集成程度更高的配置中，安讯士摄像机（可见光或热成像摄像机）还能够与IP扬声器协作，潜在地作为独立的解决方案，在侦测到相应事件时自动播放语音广播。这种类型的自动警告将推动安防措施和对策的进一步“升级”，这在判断入侵者意图以及所需的后续响应时非常重要。

APD可以直接集成到企业平台上常用的软件（如，Genetec、Milestone、SeeTec、Prysm、Qognify等）中。

安讯士提供设计补充工具，用于帮助进行调研后的规划，为项目各阶段提供支持：从根据具体要求寻找合适的产品，到准确计算存储空间要求、技术安装和系统管理。利用安讯士工具，有助于顾问规划和评估项目，并帮助集成商更顺利高效地管理项目。因为通过随附软件即可轻松安装升级包和安全补丁，这些工具甚至很容易就能保证已安装系统的安全运行。

随着威胁与对策不断演进，有一点是保持不变的，那就是：周界的完整性和安全性。对于企业负责人来说，周界安全是一项基本要务，这样才能为员工、访客和公众提供安全安心的环境。本文旨在介绍在规划周界安防的过程中，技术集成给企业带来的收益。文中还着重指出，安防技术投资应有可论证ROI的支持。在大多数情况下，对于安防从业人员来说，无论身处何部门、身兼何职、从事何种行业，了解当前的相关技术能力和未来的发展趋势都有助于保证可靠的运营安全和物资采购。

产品参考

IP热成像摄像机：

AXIS Q19等，www.axis.com/en-gb/products/thermal-cameras

分析软件：

AXIS Perimeter Defender

www.axis.com/en-gb/products/axis-perimeter-defender

外置IP扬声器：

AXIS C1310-E，www.axis.com/en-gb/products/axis-c1310-e

IP安防雷达：

D2110-VE，www.axis.com/en-gb/products/axis-d2110-ve

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