白皮书

安讯士穿戴式摄像机

系统安全

二月 2024

概述

尽管安讯士穿戴式系统基于开放平台，但它也拥有非常高的系统安全级别。

为保证摄像机丢失时的安全，摄像机建立在一个微型平台之上，其中没有不必要的软件组件。在遭受物理威胁通常较少的系统控制器中，则安置了更多功能。此外，摄像机的内部存储通过AES–256进行加密，以防数据遭到非法访问。基于IPv6和证书的通信可保证摄像机仅将数据卸载到特定的系统控制器或自身所属的系统。

在将数据从摄像机载到系统控制器时，使用的是HTTPS加密的网络连接。数据暂时存储在系统控制器的经AES–256加密的存储设备中，然后再使用其他经HTTPS加密的网络连接，进一步传输到内容目的地。

系统控制器的安全性和完整性通过符合FIPS 140–2标准的TPM（可信平台模块）进一步增强。穿戴式系统与许多其他安讯士设备共有的其他功能包括签名固件、安全启动和签名视频。

当通过AXIS Body Worn Live实时流送影像时，将在闲置、传输期间以及在观看者的网页浏览器中对数据加密。它还通过XChaCha20–Poly1305协议进行端到端加密。此外，管理员管控实时流的查看权限，这种管控细致到具体的电脑、网页浏览器和用户凭证。

目录

1 缩略词和术语

BWC： 穿戴式摄像机

VMS： 视频管理系统

EMS：证据管理系统

内容目的地： 来自（例如）穿戴式摄像机的录像和数据的存储位置。内容目的地的例子包括视频管理系统、证据管理系统和媒体服务器。

2 引言

安讯士穿戴式系统基于开放平台，能够轻松与外部系统集成以进行视频管理和证据管理。但它拥有非常高的系统安全级别，因为这是贯穿系统部署各环节的主要关注点。

本白皮书重点概述了安讯士穿戴式系统中不同组件之间的数据流动。我们尤其介绍了在从BWC录像到内容目的地的全程中，为保护系统及其数据安全所采取的措施。其中还着重介绍了不同的存储媒体，包括其他安全注意事项。

3 摄像机丢失时的安全

在日常使用中，穿戴式摄像机 (BWC) 会切实暴露于盗窃和故意破坏的风险之中。为了降低这些威胁的相关影响，采用了若干系统设计功能，以便在摄像机丢失时，也能够保证系统和数据安全。

其中一个例子是，相较于其他安讯士摄像机，BWC建立在一个微型软件平台之上，不必要的软件组件都已被移除。摄像机和系统控制器不支持VAPIX，也不支持诸如FTP、SSH或SNMP的协议。此外，摄像机也没有服务器功能。与其他系统（如VMS和EMS）的集成改为通过系统控制器来处理，相比摄像机，系统控制器遭受的物理威胁通常较少。

BWC的内部存储通过AES–256进行加密，在摄像机丢失的情况下，可防止数据遭到非法访问。

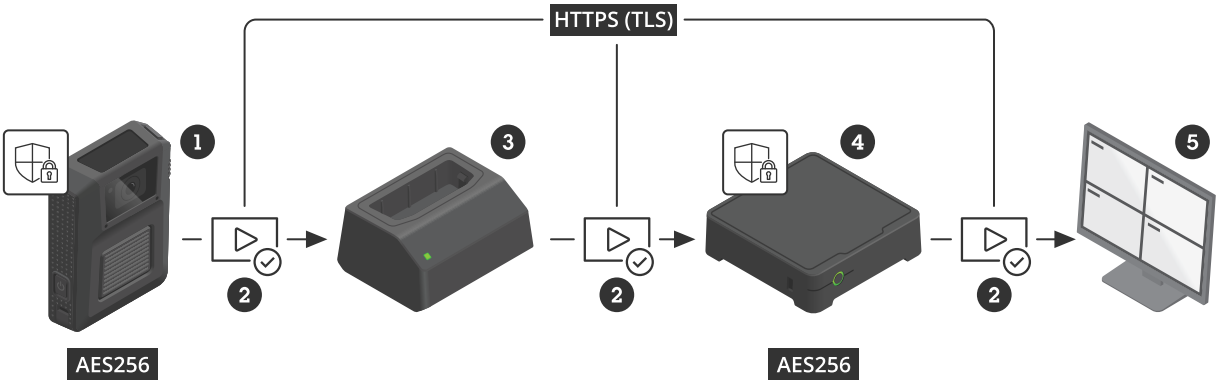
摄像机仅将数据卸载到某个特定的系统控制器或自身所属的系统。这是因为，BWC和系统控制器通过IPv6并利用证书进行通信。每当摄像机被置入扩展坞时，会自动续订证书，以匹配系统控制器的最新版本。

如果将摄像机从扩展坞中取出且与系统断开超过四周，将进入宽限期，这时系统控制器允许在八周内继续使用旧证书。如果摄像机断开超过这个时间，则需要使用主密钥口令，以手动方式重新获得系统认可。这旨在保证丢失或断开时间过长的摄像机无法在不知不觉间再次被添加，否则可能产生安全风险。

4 数据传输安全

通常，BWC在一轮工作后会置入扩展坞中，其中仍包含视频和元数据。这些数据全都通过HTTPS（HTTP与TLS的结合）加密的网络连接经由扩展坞卸载到系统控制器。数据在系统控

制器中的存储时间较短，具体存储在系统控制器的使用AES–256加密的SSD存储设备中。系统控制器随后通过HTTPS将数据传输到内容目的地。



从BWC (1) 到内容目的地 (5) 的安全数据传输和存储。

1 *配备Axis Edge Vault的BWC*
2 *签名视频（网络安全功能）*
3 *扩展坞*
4 *配备Axis Edge Vault的系统控制器*
5 *内容目的地*

如果内容目的地提供公共加密密钥，则还支持使用内容目的地的加密密钥对BWC和系统控制器中的数据加密。在这种情况下，在将数据发送至内容目的地时，数据将得到进一步强化加密。

5 其他安全功能

系统控制器的安全性和完整性通过符合FIPS 140–2标准的TPM（可信平台模块）进一步增强。

BWC和系统控制器都配备了Axis Edge Vault，它是一个基于硬件的网络安全平台，能够保护设备上的数据并实施多项安全功能。例如，通过Axis Edge Vault，可实现文件系统加密和密钥保护。*安全启动*保证设备仅可使用已授权的固件来启动。*签名固件*让设备能够在固件完整性受损的情况下，拒绝固件升级。*签名视频*通过在视频流中添加密码校验和，进一步增强了保护力度。这就让视频能够可靠回溯至生成视频的具体安讯士摄像机，确认影像未遭到篡改。

有关签名视频的更多详情，请访问*www.axis.com/developer–community/signed–video*，有关安讯士网络安全功能的更多详情，请访问*www.axis.com/solutions/built–in–cybersecurity–features*。

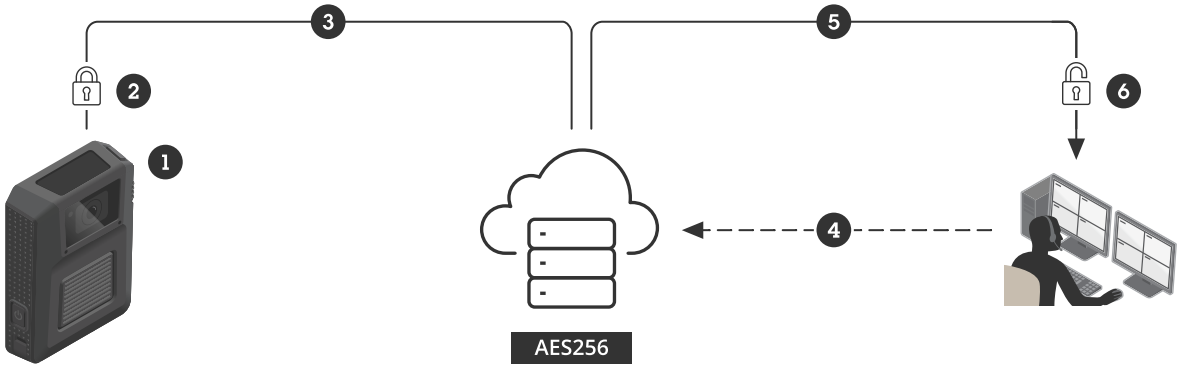
摄像机只能通过应用程序AXIS Body Worn Assistant来查看现场录像。如果启用此应用程序，BWC会将视频直接流送至此应用程序，但不会在运行此应用程序的设备的缓存或内存中存储视频资料以供日后访问。在视频流中，还进行了叠加处理，以防使用其他记录设备捕捉此视频。如果仍执行这种捕捉，则可以通过叠加数据将视频片段回溯到BWC用户。BWC的USB–C接口无法用于查看、删除或卸载视频。

6 AXIS Body Worn Live的安全保障

AXIS Body Worn Live应用程序允许访问来自安讯士穿戴式摄像机的实时数据。通过为用户提供实时视频流、音频流和其他数据流（如，位置坐标），AXIS Body Worn Live让您能够确切掌握事件的当前态势。它起先是一种基于云端的服务。

有了AXIS Body Worn Live，不仅能够在闲置（存储）和传输期间对数据进行加密，而且还能够在摄像机与观看者的网页浏览器之间对数据进行端到端加密。

所有托管在AXIS Body Worn Live中的数据和文件在闲置时使用AES–256加密。使用HTTPS通过TLS保护通信通道，采用由受信任的证书颁发机构签名的证书。AXIS Body Worn Live还使用协议XChaCha20–Poly1305添加另一层真正的端到端加密。



利用AXIS Body Worn Live中的端到端加密保证直播流传输安全

1. *BWC收集实时视频和其他数据。*
2. *在BWC中加密数据。*
3. *将数据从BWC传输到AXIS Body Worn Live。*
4. *观看者请求来自AXIS Body Worn Live的数据。*
5. *将数据从AXIS Body Worn Live流传输给观看者。*
6. *在观看者的网页浏览器中解密数据。*

穿戴式摄像机系统的管理员可全权管控实时流的查看权限。数据的加密方式使得只有经管理员批准的观看者才能够解密并查看视频，此外，管理员也可以撤销访问权限。观看者必须拥有合适的电脑、合适的网页浏览器以及合适的用户凭证。其他人（甚至包括安讯士）无法访问实时流。安讯士无法访问用户创建的端到端加密密钥。

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