# TEIL 1 ALLGEMEINES

## SYSTEMBESCHREIBUNG

### Allgemeine Anforderungen

#### Das angegebene Gerät müssen aus der offiziellen Produktlinie des Herstellers stammen und für den gewerblichen und/oder industriellen Einsatz rund um die Uhr ausgelegt sein.

#### Das angegebene Gerät basiert auf Standardkomponenten und bewährter Technologie unter Verwendung offener und veröffentlichter Protokolle.

### Nachhaltigkeit

#### Das angegebene Gerät muss gemäß ISO 14001 hergestellt sein.

#### Das angegebene Gerät muss den EU-Richtlinien 2011/65/EU (RoHS) und 2012/19/EU entsprechen (WEEE).

#### Das angegebene Gerät muss der EU-Verordnung 1907/2006 entsprechen (REACH).

## ZERTIFIZIERUNGEN UND STANDARDS

### Allgemeine Abkürzungen und Akronyme

#### AES: fortgeschrittener Verschlüsselungsstandard (Advanced Encryption Standard)

#### API: Anwendungsprogrammierschnittstelle (Application Programming Interface)

#### Bitrate: die Anzahl der über ein Netzwerk gesendeten Bits/Zeiteinheiten

#### DHCP: Protokoll der dynamischen Hostkonfiguration (Dynamic Host Configuration Protocol)

#### DNS: Domainnamensystem (Domain Name System)

#### FPS: Bilder pro Sekunde (Frames per Second)

#### FTP: Dateiübertragungsprotokoll (File Transfer Protocol)

#### H.264 (Videokomprimierungsformat)

#### IEEE 802.1x: Authentisierungs-Rahmenwerk für Netzwerkgeräte

#### IP: Internetprotokoll (Internet Protocol)

#### IR-Licht: Infrarotlicht

#### ISO: Organisation für internationale Standards (International Standards Organization)

#### JPEG: Gemeinsame fotografische Expertengruppe (Joint Photographic Experts Group) (Bildformat)

#### LAN: Lokales Netzwerk (Local Area Network)

#### LED: Leuchtdiode (Light Emitting Diode)

#### MPEG: Expertengruppe für bewegte Bilder (Moving Picture Experts Group)

#### Multicast: Kommunikation zwischen einem einzelnen Sender und mehreren Empfängern in einem Netzwerk

#### NTP: Netzwerkzeitprotokoll (Network Time Protocol)

#### ONVIF: Globaler Standard für die Schnittstelle von IP-basierten physischen Sicherheitsprodukten

#### PACS: Physisches Zugangskontrollsystem (Physical Access Control System)

#### PoE: Power over Ethernet (IEEE 802.3af/at) Standard für die Bereitstellung von Strom über Netzwerkkabel

#### Progressiver Scan: Eine Bildscantechnologie, die das gesamte Bild scannt

#### QoS: Servicequalität (Quality of Service)

#### RPC: Fernprozeduranruf (Remote Procedure Call)

#### SIP: Gesprächsprotokoll (Session Initiation Protocol)

#### SMTP: Einfaches Mail-Übertragungsprotokoll (Simple Mail Transfer Protocol)

#### SNMP: Einfaches Netzwerkverwaltungsprotokoll (Simple Network Management Protocol)

#### SSL: Sichere Steckdosenschicht (Secure Sockets Layer)

#### TCP: Übertragungssteuerungsprotokoll (Transmission Control Protocol)

#### TLS: Transportschicht-Sicherheit (Transport Layer Security)

#### Unicast: Kommunikation zwischen einem einzelnen Sender und einem einzelnen Empfänger in einem Netzwerk

#### UPS: Unterbrechungsfreie Stromversorgung (Uninterruptible Power Supply)

#### VBR: Variable Bitrate (Variable Bit Rate)

#### VMS: Videomanagementsystem (Video Management System)

#### WDR: Große dynamische Reichweite (Wide dynamic range)

### Das angegebene Gerät müssen die folgenden EMV-Zulassungen besitzen:

#### EN55032: 2012

#### EN55024: 2010

#### 2014/35/EU

#### 2014/30/EU

#### 2012/19/EU

#### 2011/65/EU

#### EN 55032 Klasse A

#### EN 55032 Klasse B

#### EN 55024

#### FCC Teil 15 - Unterabschnitt B Klasse A

#### FCC Teil 15 - Unterabschnitt B Klasse B

#### FCC Teil 15 - Unterabschnitt B Klasse A + B

#### ICES-003 Klasse A

#### ICES-003 Klasse B

### Das angegebene Gerät müssen den folgenden Produktsicherheitsstandards entsprechen:

#### IEC/EN/UL 60950-1

### Das angegebene Gerät müssen die folgenden Standards erfüllen

#### Audio:

##### G.711

##### G.729

##### G.722 (Breitband)

##### L16 / 16kHz (Breitband)

#### Video:

##### H.263+

##### H.263

##### H.264 (MPEG-4 AVC)

##### MPEG-4 Teil 2

##### MJPEG

#### Vernetzung:

##### IEEE 802.3af/802.3at (Power over Ethernet)

##### IEEE 802.1X (Authentifizierung)

##### IPv4 (RFC 791)

##### QoS

#### Mechanische Umgebung:

##### IEC/EN 60529 IP65

##### IEC/EN 62262 IK07

## QUALITÄTSSICHERUNG

### Der Auftragnehmer bzw. Sicherheitssubunternehmer ist ein lizenzierter Sicherheitsauftragnehmer mit mindestens fünf (5) Jahren Erfahrung in der Installation und Wartung von Systemen mit ähnlichem Umfang und ähnlicher Komplexität und mit dem Nachweis, dass mindestens drei (3) Projekte ähnlicher Bauart von ihm abgeschlossen wurden und dass er derzeit mit der Installation und Wartung der hier beschriebenen Systeme befasst ist.

### Alle Installations-, Konfigurations-, Einrichtungs-, Programm- und damit verbundene Arbeiten müssen von Elektronikern durchgeführt werden, die vom Hersteller gründlich in der Installation und Wartung der bereitgestellten Geräte geschult wurden.

### Der Auftragnehmer oder ein benannter Subunternehmer muss als Nachweis des Wissens die von einer Drittorganisation überprüften Zeugnisse der abgeschlossenen Herstellerzertifizierung vorlegen.

### Der Auftragnehmer stellt vier (4) aktuelle Referenzen von Kunden mit Systemen ähnlichen Umfangs und ähnlicher Komplexität zur Verfügung, die in den letzten drei (3) Jahren in Betrieb genommen wurden. Mindestens drei (3) dieser Referenzen müssen dieselben Systemkomponenten in einer ähnlichen Konfiguration wie das vorgeschlagene System verwenden.

### Das angegebene Gerät müssen gemäß ISO9001 hergestellt sein.

## GARANTIE

### Für alle vom Auftragnehmer bereitgestellten Sicherheitssystemkomponenten und Arbeitskräfte, einschließlich Verkabelung, Software, Hardware und kundenspezifischer Teile, wird eine Garantie von mindestens drei (3) Jahren für Teile, Materialien, Arbeits- und Reisekosten gewährt.

### Der Hersteller gewährt für das Gerät eine Garantie und optional eine erweiterte Garantie für einen Gesamtzeitraum von maximal fünf Jahren. Wenn dies im Rahmen des Vertrags festgelegt wird, repariert oder ersetzt der Auftragnehmer Teile und/oder Arbeitskräfte gemäß der Garantie für die Dauer dieser Garantie, ohne dass hierfür Kosten für den Kunden anfallen.

# TEIL 2 PRODUKTE

## 2.01 ALLGEMEINES

### Die Gegensprechanlagen müssen IP-basiert sein und den festgelegten Netzwerk- und Videostandards entsprechen.

### Die Gegensprechanlagen müssen über den Schalter mit dem Netzwerkkabel mit Strom versorgt werden.

### Die Gegensprechanlagen müssen vollständig von einer offenen und veröffentlichten API (Application Programmers Interface) unterstützt werden, die die erforderlichen Informationen für die Integration von Funktionen in Anwendungen von Drittanbietern bereitstellt.

## 2.02 Zeitplan der GEGENSPRECHANLAGEN

### Die unten aufgeführten Gegensprechanlagen-Typen, die verschiedene Auflösungen, Formfaktoren und Merkmale beschreiben, müssen von einem einzigen Gegensprechanlagen-Hersteller geliefert werden.

### Die Hersteller- und Modellnummern der Gegensprechanlage lauten wie folgt:

#### Die modulare IP-Gegensprechanlage muss eine 2N IP-Basis mit Kamera sein.

## 2.03 Gegensprechanlage

### Die modulare IP-Gegensprechanlage

#### Die Gegensprechanlage muss die folgenden Konstruktionsspezifikationen erfüllen oder übertreffen:

##### Die Gegensprechanlage muss einen eingebauten Webserver enthalten.

##### Die Gegensprechanlage muss in der Lage sein, definierte lokale Zugriffssteuerungsfunktionen auszuführen, ohne mit dem Netzwerk verbunden zu sein.

##### Die Gegensprechanlage soll die Option zum Hinzufügen eingebetteter RFID-Lesegeräte unterstützen.

#### Die Gegensprechanlage muss die folgenden Leistungsspezifikationen erfüllen oder übertreffen:

##### Video

###### Die Gegensprechanlage muss Videostreams in 640 x 480 mit bis zu 30 Bildern pro Sekunde mit H.264, H.263, H.263 + oder mit MJPEG mit bis zu 15 Bildern pro Sekunde bereitstellen.

###### Die Kamera der Gegensprechanlage muss Bilder in Auflösungen von bis zu 1280 x 960 liefern.

###### Die Gegensprechanlage muss die folgenden Videokodierungsalgorithmen unterstützen:

H.263+

H.263

H.264

MPEG-4 Part 2

MJPEG

###### Die Gegensprechanlage muss unabhängig konfigurierte simultane H.264- und MJPEG-Streams bereitstellen.

###### Die Gegensprechanlage soll in H.263, H.263, H.264 die konstante Bitrate (CBR) unterstützen, um das Netzwerk vor unerwarteten Bitraten-Spitzen zu schützen.

###### Die Gegensprechanlage muss konfigurierbare Komprimierungsstufen bereitstellen.

###### Unterstützung des Standard-Basislinienprofils H.264 mit Bewegungsschätzung.

###### Unterstützung der Bewegungsschätzung in H.264 / MPEG-4 Part 10 / AVC.

###### Die Gegensprechanlage muss den Transport von Videos ermöglichen:

HTTP (Unicast)

HTTPS (Unicast)

RTP (Unicast & Multicast)

RTP durch RTSP (Unicast)

RTP durch RTSP durch HTTP (Unicast)

###### Die Gegensprechanlage muss Servicequalität (QoS) unterstützen, um den Verkehr priorisieren zu können.

##### Bild

###### Die Kamera muss einen automatischen Weißabgleich enthalten.

###### Die Kamera muss manuell definierte Werte für Folgendes unterstützen:

Farbstufe

Helligkeit

##### Audio

###### Die Gegensprechanlage muss Zwei-Wege-Vollduplex-Audio unterstützen:

Eingabequellen

interne Mikrofon

Ausgabequellen

Eingebauter Lautsprecher, 2W

###### Die Gegensprechanlage muss separat einstellbare Lautstärkepegel für Folgendes unterstützen:

Anruf

Schlüssel

Klingeltöne

Vorinstallierte Audioclips

Warntöne

Paging

###### Die Gegensprechanlage muss die adaptive Verstärkungsregelung unterstützen.

###### Kodierung

Die Gegensprechanlage soll Folgendes unterstützen:

G.711

G.722 (Breitband)

G.729

L16 / 16kHz (Breitband)

###### Die Gegensprechanlage muss einen Schalldruckpegel von mindestens 78 dB bei 1 kHz bei 1 m liefern.

###### Die Gegensprechanlage muss mit einer aktiven Echokompensation ausgestattet sein.

###### Die Gegensprechanlage muss die Audio-Übertragung durch Folgendes ermöglichen:

RTP (Unicast & Multicast)

RTP durch RTSP (Unicast)

RTP durch RTSP durch HTTP (Unicast)

###### Die Gegensprechanlage muss Servicequalität (QoS) unterstützen, um den Verkehr priorisieren zu können.

##### Anruffunktionalität

###### Die Gegensprechanlage muss SIP für die Integration in VoIP, Peer-to-Peer unterstützen oder in SIP/PBX integriert sein.

###### Die Gegensprechanlage muss die Verwendung von SIP-Proxy unterstützen, der mit dem SIP-Registrar für ausgehende Anrufe identisch sein kann.

###### Die Gegensprechanlage unterstützt das Wählen von bis zu zwölf separaten Nummern in Folge oder als Ringgruppe.

##### Zugriffssteuerungsfunktionalität

###### Die Ausgänge der Gegensprechanlagen müssen die Fernbedienung mithilfe von DTMF-Codes unterstützen.

###### Jeder Benutzer muss eindeutige Zugangscodes für jede elektrische Ausgabe haben.

##### Benutzeroberfläche

###### Webserver

Die Gegensprechanlage muss einen integrierten Webserver enthalten, der mehreren Kunden in einer Standardbetriebssystem- und Browserumgebung über HTTP Funktionalität und Konfiguration zur Verfügung stellt, ohne dass zusätzliche Software erforderlich ist.

###### Sprachspezifikation

Die Gegensprechanlage muss eine Funktion zum Ändern der Sprache der Benutzeroberfläche bereitstellen, mindestens 7 verschiedene Sprachen unterstützen und die Möglichkeit bieten, eine zusätzliche Sprache durch Anpassung zu unterstützen.

###### IP-Adressen

Die Gegensprechanlage muss sowohl feste IP-Adressen als auch dynamisch zugewiesene IP-Adressen unterstützen, die von einem DHCP-Dienst (Dynamic Host Control Protocol) bereitgestellt werden.

Die Gegensprechanlage muss die automatische Erkennung der Gegensprechanlage basierend auf WS Discovery ermöglichen, wenn ein Computer mit einem Betriebssystem verwendet wird, das diese Funktion unterstützt.

Die Gegensprechanlage unterstützt IPv4.

##### Ereignisfunktionalität

###### Die Gegensprechanlage muss mit einer integrierten Ereignisfunktionalität ausgestattet sein, die durch Folgendes ausgelöst werden kann:

Manipulation / offen

SIP Anrufstatus inkl. des eingehenden Anrufs

Änderung des SIP-Registrierungsstatus

Video-Bewegungserkennung

Geräuscherkennung

SIP-DTMF-Sequenzen

Externe Eingabe

Zugriffskontrollereignisse wie die eingegebene Karte

Vordefinierte Zeit

###### Die Reaktion auf Auslöser umfasst Folgendes:

eine Benachrichtigung über HTTP oder E-Mail senden

Tonalarm aktivieren

Anruf machen oder beenden

eine Benachrichtigung über HTTP, HTTPS, Wiegand oder E-Mail senden

Bilder per FTP oder E-Mail senden

externen Ausgang aktivieren

Audioclip abspielen

##### Protokoll

###### Die Gegensprechanlage muss mindestens für Folgendes Unterstützung enthalten: HTTP, HTTPS, SIP 2.0, TFTP, RTSP, RTP, SMTP, DHCP opt 66, NTP, Syslog.

###### Die SMTP-Implementierung muss die SMTP-Authentifizierung unterstützen.

###### Die Kamera muss mindestens IPv4, HTTP, HTTPS, SIP, SSL/TLS, QoS-Schicht-3-DiffServ, TCP, ICMP, SNMPv2c, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, ARP, DNS, NTP unterstützen,

##### Sicherheit

###### Die Gegensprechanlage soll die Verwendung von HTTPS und SSL/TLS unterstützen und die Möglichkeit bieten, signierte Zertifikate hochzuladen, um die Authentifizierung und Kommunikation von Verwaltungsdaten und Video-Streams zu verschlüsseln und zu sichern.

###### Die Gegensprechanlage blockiert ihre Anmeldeseite für 30 Sekunden, nachdem drei fehlerhafte Passwörter übermittelt wurden.

###### Die Gegensprechanlage zwingt den Benutzer, das Administratorkennwort bei der ersten Installation zu ändern.

###### Die Gegensprechanlage bietet eine zentralisierte Zertifikatsverwaltung mit der Möglichkeit, CA-Zertifikate hochzuladen. Die Zertifikate müssen von einer Organisation unterzeichnet werden, die digitale Vertrauensdienste anbietet.

###### Die Gegensprechanlage unterstützt die IEEE 802.1X-Authentifizierung.

###### Ausgewählte Dienste wie RTSP oder Webkonfiguration müssen so konfigurierbar sein, dass nur der Zugriff von lokalen Geräten möglich ist.

###### Die Gegensprechanlage beschränkt den Zugriff auf den integrierten Webserver durch Benutzername und Passwort.

###### Die Gegensprechanlage muss mit der Option einer Manipulationserkennung ausgestattet sein.

##### API-Unterstützung

###### Die Gegensprechanlage muss vollständig von einer offenen und veröffentlichten API (Application Programmers Interface) unterstützt werden, die die erforderlichen Informationen für die Integration von Funktionen in Anwendungen von Drittanbietern bereitstellt.

###### Die Gegensprechanlage muss dem von der ONVIF-Organisation definierten ONVIF-Profil S entsprechen.

Informationen zu den ONVIF-Profilspezifikationen finden Sie unter [www.onvif.org/](http://galaxis.axis.com/PartnerPortal/AE/Documents/internal/ae-spec_templates/www.onvif.org)

###### Die Gegensprechanlage muss mit den wichtigsten PBX- und Gateway-Herstellern interoperabel/zertifiziert sein, einschließlich:

Cisco

Avaya

Broadsoft

##### Installation und Wartung

###### Die Gegensprechanlage muss eine sichere Konfiguration mit HTTPS unterstützen.

###### Die Gegensprechanlage soll die Verwendung von SNMP-basierten Verwaltungstools gemäß SNMP v2c unterstützen.

###### Die Gegensprechanlage ermöglicht Aktualisierungen der Software (Firmware) über das Netzwerk unter Verwendung von TFTP, HTTP oder Webschnittstelle.

###### Die Gegensprechanlage akzeptiert die externe Zeitsynchronisation von einem NTP-Server (Network Time Protocol).

###### Die Gegensprechanlage unterstützt das Sichern und Wiederherstellen der Konfiguration.

###### Die Gegensprechanlage speichert alle kundenspezifischen Einstellungen in einem nichtflüchtigen Speicher, der bei Stromausfällen oder Soft-Reset nicht verloren gehen darf.

##### Zugriffsprotokoll

###### Die Gegensprechanlage muss in der Lage sein, Ereignisse wie Codes, Telefonanrufe, RFID-Karten usw. zu protokollieren und über die HTTP-Schnittstelle zur Überwachung bereitzustellen.

###### Der Administrator muss festlegen können, ob die bestimmten Nachrichten unmittelbar nach dem Eintreten eines Ereignisses von der Gegensprechanlage gesendet werden oder ob sich der Kunde für die Ereignisprotokollierung registriert und dann seit der letzten Registrierung alle Ereignisse gleichzeitig anfordert.

###### Der Kunde muss auswählen können, welche Nachrichten aus dem Ereignisprotokoll gemeldet werden.

##### Gegensprechanlage-Diagnostik

###### Die Gegensprechanlage muss mit LED-Leuchten ausgestattet sein, die sichtbare Statusinformationen liefern können. Die LED-Leuchten zeigen den Betriebsstatus der Gegensprechanlage an und geben Auskunft über Stromversorgung, Netzwerkstatus und Gegensprechanlagenstatus.

###### Die Gegensprechanlage muss von einer Wachhundfunktion überwacht werden, die Prozesse automatisch neu initiiert oder das Gerät neu startet, wenn eine Fehlfunktion festgestellt wird.

##### Hardware-Schnittstellen

###### Netzwerkschnittstelle

Die Gegensprechanlage muss mit einem 10BASE-T/100BASE-TX Fast Ethernet-Port ausgestattet sein, der einen Standard-RJ45-Anschluss verwendet, und die automatische Aushandlung der Netzwerkgeschwindigkeit (100 MBit/s und 10 MBit/s) und des Übertragungsmodus (Voll- und Halbduplex) unterstützen.

###### Türe

Die Gegensprechanlage muss mit einem programmierbaren Eingang ausgestattet sein, der sowohl die Kurzschlussaktivierung als auch bis zu +30 VDC für die Türüberwachung oder die Forderung zum Beenden (REX) unterstützt.

Die Gegensprechanlage muss mit zwei unabhängigen Ausgängen zur Türsteuerung ausgestattet sein. Ein aktives Relais mit mindestens 8 VDC/600 mA und ein Schließerrelais/Öffnerrelais, das bis zu 30 V AC/DC 1A unterstützt.

###### Leistung

Die Gegensprechanlage muss mit einem abnehmbaren Klemmenblock ausgestattet sein, der die Konnektivität für die externe Stromversorgung gewährleistet.

##### Anlage

###### Die Gegensprechanlage soll:

mit IP65-Gehäuse hergestellt und IK07-zertifiziert werden

mit einem Sabotageschalter ausgestattet sein.

mit schwarzer Oberfläche erhältlich sein.

##### Leistung

###### Stromversorgung über Ethernet IEEE 802.3af / 802.3at Typ 1 Klasse 0

###### 12 V DC

max: 2A

##### Umwelt

###### Die Gegensprechanlage soll:

im folgenden Temperaturbereich arbeiten -40 °C bis +55 °C (-40 °F bis 131 °F)

in einem Luftfeuchtigkeitsbereich von 10-95 % relativer Luftfeuchtigkeit (nicht kondensierend) arbeiten.

# TEIL 3 AUSFÜHRUNG

## 3.01 installation

### Der Auftragnehmer muss die Anweisungen in der vom Hersteller bereitgestellten Dokumentation sorgfältig befolgen, um sicherzustellen, dass alle Schritte unternommen wurden, um ein zuverlässiges, einfach zu bedienendes System bereitzustellen.

### Alle Geräte müssen vor der Installation gemäß den Anweisungen des Herstellers geprüft und konfiguriert werden.

### Die gesamte Firmware, die in den Produkten enthalten ist, muss die neueste und aktuellste Firmware sein, die vom Hersteller bereitgestellt wird.

### Alle Geräte, bei denen die Benutzer sich mit einem Kennwort anmelden müssen, müssen mit benutzer-/standortspezifischen Kennwörtern konfiguriert sein. System-/ Produkt-Standardkennwörter sind nicht zulässig.

ENDE DES ABSCHNITTS