

WHITE PAPER

Quick guide to Axis datasheets

Approvals, certifications, and protocols

November 2021

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 3 |
| 2 | Approvals | 3 |
| | 2.1 EMC (Electromagnetic compatibility) | 3 |
| | 2.2 Safety | 4 |
| | 2.3 Environment | 5 |
| | 2.4 Other approvals | 8 |
| 3 | Certifications | 8 |
| 4 | Power | 9 |
| | 4.1 Power over Ethernet (PoE) classes | 9 |
| 5 | Network | 10 |
| | 5.1 Protection and security control | 10 |
| | 5.2 Supported protocols | 10 |

1 Introduction

Axis Communications adheres to the applicable industry standards and compliance standards for all products that are brought to market. This document supplements Axis datasheets with definitions and short descriptions of acronyms, approvals, certifications, and protocols found therein.

This document provides information about the datasheet sections that are highlighted and zoomed in below.

| AXIS P5654-E PTZ Network Camera | |
|--|--|
| Model | AXIS P5654-E 60 Hz AXIS P5654-E 60 Hz |
| Image sensor | 1/2" progressive scan CMOS |
| Lens | Varifocal, 4.0-84.8 mm, F1.6 - 4.5 Horizontal field of view: 77.0° - 1.6° Vertical field of view: 43.1° - 2.0° Autofocus and auto-iris |
| Day and night | Automatically removable infrared-cut filter |
| Minimum illumination | Color: 0.1 lux at 30 IR, F1.6 BW: 0.03 lux at 50 IR F1.6 BW: 0.01 lux at 30 IR F1.6 |
| Shutter speed | 1/60000 s to 2 s |
| Pan/Tilt/Zoom | Pan: 180° endless, 0.1° - 360°/s Tilt: 180° - 0.1° - 360°/s Zoom: 21x optical, 12x digital, total 252x zoom 25x preset position, e-iris, limited guard band control zones, on-screen directional indicators, set new pan 0°, focus window, focus reset |
| System on Chip (SoC) | |
| Model | ARMV7-C |
| Memory | 1024 MB RAM, 512 MB Flash |
| Compute capabilities | Machine learning processing unit (MLPU) |
| Video | |
| Video compression | H.264 (MP@4 Part 10/AVC) Baseline, Main and High Profiles H.265 (MP@L4 Part 10/AVC) Main Profile Motion JPEG |
| Resolution | 1280x720 H265 75FPS to 3264x1840 |
| Frame rate | Up to 60FPS for 1080P H264 in all resolutions |
| Video streaming | Multiple, individually configurable streams in H.264, H.265 and Motion JPEG Controllable frame rate and bandwidth Axis Streamer technology in H.264 and H.265 VBv4/AMR in H.264/1280 |
| Image settings | Compression, saturation, brightness, sharpness, contrast, local contrast, white balance, exposure control, exposure zones, Forensic WDR: Up to 120 dB depending on scene, deblurring, day/night level, zone mapping, face zoning of low-light behavior, rotation: 0°, 180°, iris and image overlay, image freeze on PTZ, electronic image stabilization, scene profiles, 20 individual polygon privacy masks |
| Network | |
| Security | Secure operations: secure boot, secure updates, secure boot, IEEE 802.1X network access control, digest authentication, user access log, central log certificate management, brute force delay protection, signed firmware, secure boot |
| Supported protocols | IPv4, IPv6, USGv6, HTTP, HTTPS, SMTP, Bonjour, UPnP, S/NMP v1/v2/v3 (MIB-II), DNS, DynDNS, NTP, RTP, SRTP, TCP, UDP, ICMPv4/v6, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, NTPv2, LLDP, CDP, MQTT v3.1.1, Syslog |
| System integration | Open API for software integration, including VADP and AXIS Camera Application Platform, specifications at axis.com |
| Application Programming Interface | ONVIF Profile G, ONVIF Profile S, and ONVIF Profile T, specifications at onvif.org |
| Event conditions | Device status: Above operating temperature, Above or below operating temperature, Below operating temperature, Fan failure, IP address removal, Network lost, New IP address, Shock detected, Storage failure, System ready, Within operating temperature, Edge storage, Streaming ongoing, Storage disconnection I/O: Manual trigger, Virtual input PTZ: PTZ malfunctioning, PTZ movement: Camera 1, PTZ preset position reached, Camera 1, PTZ ready Scheduled and recurring: Scheduled event |
| Event actions | Day-night mode, go to preset position, guard tour, upload of images or video data via FTP, SFTP, HTTP, HTTPS, network share and email, notification to email, HTTP, HTTPS, TCP and SNMP trap, twofax start, authorized direct, record video to SD card and network share, WDR mode |
| Data streaming | Event data |
| Basic installation aids | Fast connector |
| Identifiers | |
| AXIS Object Analytics | Object classes: humans, vehicles Trigger conditions: line crossing, object in area Up to 10 scenarios Markers visualized with color-coded bounding boxes Polygons include/exclude areas Perspective configuration ONVIF Motion Alarm event |
| Applications | Included AXIS Object Analytics AXIS Video Motion Detection, advanced antipeeper, autostracker 2 Support for AXIS Camera Application Platform enabling installation of third-party applications, see axis.com/ocap |
| Casing | IP66, NEMA 4X and R10 Aluminum anodized polycarbonate (PC) dome Color: anodized PC is 7000-B, replaceable slide cover For mounting instructions of casing and impact on warranty, contact your Axis partner |
| Sustainability | PVC free AXIS PoE+ midspan 1-port: 100-240 V AC, max 37 W IEEE 802.3at, Type 2 Class 4 Camera consumption: typical 8 W, max 16 W (PoE+ midspan not included) |
| Connectors | RJ45 10BASE-T/100BASE-TX ICE RJ45 push-pull connector (PSE) not included Support for SD card encryption (AES-128/256bit) Recording to network-attached storage (NAS) For SD card and NAS recommendations see axis.com |
| Operating conditions | +20 °C to +50 °C (68 °F to 122 °F) Maximum ambient temperature +55°C Humidity: 0-100% RH (non-condensing) |
| Storage conditions | -40 °C to 65 °C (-40 °F to 149 °F) Humidity: 5-95% RH (non-condensing) |
| Approvals | EMC EN 61010-1, EN 61010-2, EN 61010-3, EN 61010-4 EN 50524-2, EN 50524-3, EN 50524-4 EN 50524-5, EN 50524-6 EN 50524-7, EN 50524-8 EN 50524-9, EN 50524-10 EN 50524-11, EN 50524-12 EN 50524-13, EN 50524-14 EN 50524-15, EN 50524-16 EN 50524-17, EN 50524-18 EN 50524-19, EN 50524-20 EN 50524-21, EN 50524-22 EN 50524-23, EN 50524-24 EN 50524-25, EN 50524-26 EN 50524-27, EN 50524-28 EN 50524-29, EN 50524-30 EN 50524-31, EN 50524-32 EN 50524-33, EN 50524-34 EN 50524-35, EN 50524-36 EN 50524-37, EN 50524-38 EN 50524-39, EN 50524-40 EN 50524-41, EN 50524-42 EN 50524-43, EN 50524-44 EN 50524-45, EN 50524-46 EN 50524-47, EN 50524-48 EN 50524-49, EN 50524-50 EN 50524-51, EN 50524-52 EN 50524-53, EN 50524-54 EN 50524-55, EN 50524-56 EN 50524-57, EN 50524-58 EN 50524-59, EN 50524-60 EN 50524-61, EN 50524-62 EN 50524-63, EN 50524-64 EN 50524-65, EN 50524-66 EN 50524-67, EN 50524-68 EN 50524-69, EN 50524-70 EN 50524-71, EN 50524-72 EN 50524-73, EN 50524-74 EN 50524-75, EN 50524-76 EN 50524-77, EN 50524-78 EN 50524-79, EN 50524-80 EN 50524-81, EN 50524-82 EN 50524-83, EN 50524-84 EN 50524-85, EN 50524-86 EN 50524-87, EN 50524-88 EN 50524-89, EN 50524-90 EN 50524-91, EN 50524-92 EN 50524-93, EN 50524-94 EN 50524-95, EN 50524-96 EN 50524-97, EN 50524-98 EN 50524-99, EN 50524-100 EN 50524-101, EN 50524-102 EN 50524-103, EN 50524-104 EN 50524-105, EN 50524-106 EN 50524-107, EN 50524-108 EN 50524-109, EN 50524-110 EN 50524-111, EN 50524-112 EN 50524-113, EN 50524-114 EN 50524-115, EN 50524-116 EN 50524-117, EN 50524-118 EN 50524-119, EN 50524-120 EN 50524-121, EN 50524-122 EN 50524-123, EN 50524-124 EN 50524-125, EN 50524-126 EN 50524-127, EN 50524-128 EN 50524-129, EN 50524-130 EN 50524-131, EN 50524-132 EN 50524-133, EN 50524-134 EN 50524-135, EN 50524-136 EN 50524-137, EN 50524-138 EN 50524-139, EN 50524-140 EN 50524-141, EN 50524-142 EN 50524-143, EN 50524-144 EN 50524-145, EN 50524-146 EN 50524-147, EN 50524-148 EN 50524-149, EN 50524-150 EN 50524-151, EN 50524-152 EN 50524-153, EN 50524-154 EN 50524-155, EN 50524-156 EN 50524-157, EN 50524-158 EN 50524-159, EN 50524-160 EN 50524-161, EN 50524-162 EN 50524-163, EN 50524-164 EN 50524-165, EN 50524-166 EN 50524-167, EN 50524-168 EN 50524-169, EN 50524-170 EN 50524-171, EN 50524-172 EN 50524-173, EN 50524-174 EN 50524-175, EN 50524-176 EN 50524-177, EN 50524-178 EN 50524-179, EN 50524-180 EN 50524-181, EN 50524-182 EN 50524-183, EN 50524-184 EN 50524-185, EN 50524-186 EN 50524-187, EN 50524-188 EN 50524-189, EN 50524-190 EN 50524-191, EN 50524-192 EN 50524-193, EN 50524-194 EN 50524-195, EN 50524-196 EN 50524-197, EN 50524-198 EN 50524-199, EN 50524-200 EN 50524-201, EN 50524-202 EN 50524-203, EN 50524-204 EN 50524-205, EN 50524-206 EN 50524-207, EN 50524-208 EN 50524-209, EN 50524-210 EN 50524-211, EN 50524-212 EN 50524-213, EN 50524-214 EN 50524-215, EN 50524-216 EN 50524-217, EN 50524-218 EN 50524-219, EN 50524-220 EN 50524-221, EN 50524-222 EN 50524-223, EN 50524-224 EN 50524-225, EN 50524-226 EN 50524-227, EN 50524-228 EN 50524-229, EN 50524-230 EN 50524-231, EN 50524-232 EN 50524-233, EN 50524-234 EN 50524-235, EN 50524-236 EN 50524-237, EN 50524-238 EN 50524-239, EN 50524-240 EN 50524-241, EN 50524-242 EN 50524-243, EN 50524-244 EN 50524-245, EN 50524-246 EN 50524-247, EN 50524-248 EN 50524-249, EN 50524-250 EN 50524-251, EN 50524-252 EN 50524-253, EN 50524-254 EN 50524-255, EN 50524-256 EN 50524-257, EN 50524-258 EN 50524-259, EN 50524-260 EN 50524-261, EN 50524-262 EN 50524-263, EN 50524-264 EN 50524-265, EN 50524-266 EN 50524-267, EN 50524-268 EN 50524-269, EN 50524-270 EN 50524-271, EN 50524-272 EN 50524-273, EN 50524-274 EN 50524-275, EN 50524-276 EN 50524-277, EN 50524-278 EN 50524-279, EN 50524-280 EN 50524-281, EN 50524-282 EN 50524-283, EN 50524-284 EN 50524-285, EN 50524-286 EN 50524-287, EN 50524-288 EN 50524-289, EN 50524-290 EN 50524-291, EN 50524-292 EN 50524-293, EN 50524-294 EN 50524-295, EN 50524-296 EN 50524-297, EN 50524-298 EN 50524-299, EN 50524-300 EN 50524-301, EN 50524-302 EN 50524-303, EN 50524-304 EN 50524-305, EN 50524-306 EN 50524-307, EN 50524-308 EN 50524-309, EN 50524-310 EN 50524-311, EN 50524-312 EN 50524-313, EN 50524-314 EN 50524-315, EN 50524-316 EN 50524-317, EN 50524-318 EN 50524-319, EN 50524-320 EN 50524-321, EN 50524-322 EN 50524-323, EN 50524-324 EN 50524-325, EN 50524-326 EN 50524-327, EN 50524-328 EN 50524-329, EN 50524-330 EN 50524-331, EN 50524-332 EN 50524-333, EN 50524-334 EN 50524-335, EN 50524-336 EN 50524-337, EN 50524-338 EN 50524-339, EN 50524-340 EN 50524-341, EN 50524-342 EN 50524-343, EN 50524-344 EN 50524-345, EN 50524-346 EN 50524-347, EN 50524-348 EN 50524-349, EN 50524-350 EN 50524-351, EN 50524-352 EN 50524-353, EN 50524-354 EN 50524-355, EN 50524-356 EN 50524-357, EN 50524-358 EN 50524-359, EN 50524-360 EN 50524-361, EN 50524-362 EN 50524-363, EN 50524-364 EN 50524-365, EN 50524-366 EN 50524-367, EN 50524-368 EN 50524-369, EN 50524-370 EN 50524-371, EN 50524-372 EN 50524-373, EN 50524-374 EN 50524-375, EN 50524-376 EN 50524-377, EN 50524-378 EN 50524-379, EN 50524-380 EN 50524-381, EN 50524-382 EN 50524-383, EN 50524-384 EN 50524-385, EN 50524-386 EN 50524-387, EN 50524-388 EN 50524-389, EN 50524-390 EN 50524-391, EN 50524-392 EN 50524-393, EN 50524-394 EN 50524-395, EN 50524-396 EN 50524-397, EN 50524-398 EN 50524-399, EN 50524-400 EN 50524-401, EN 50524-402 EN 50524-403, EN 50524-404 EN 50524-405, EN 50524-406 EN 50524-407, EN 50524-408 EN 50524-409, EN 50524-410 EN 50524-411, EN 50524-412 EN 50524-413, EN 50524-414 EN 50524-415, EN 50524-416 EN 50524-417, EN 50524-418 EN 50524-419, EN 50524-420 EN 50524-421, EN 50524-422 EN 50524-423, EN 50524-424 EN 50524-425, EN 50524-426 EN 50524-427, EN 50524-428 EN 50524-429, EN 50524-430 EN 50524-431, EN 50524-432 EN 50524-433, EN 50524-434 EN 50524-435, EN 50524-436 EN 50524-437, EN 50524-438 EN 50524-439, EN 50524-440 EN 50524-441, EN 50524-442 EN 50524-443, EN 50524-444 EN 50524-445, EN 50524-446 EN 50524-447, EN 50524-448 EN 50524-449, EN 50524-450 EN 50524-451, EN 50524-452 EN 50524-453, EN 50524-454 EN 50524-455, EN 50524-456 EN 50524-457, EN 50524-458 EN 50524-459, EN 50524-460 EN 50524-461, EN 50524-462 EN 50524-463, EN 50524-464 EN 50524-465, EN 50524-466 EN 50524-467, EN 50524-468 EN 50524-469, EN 50524-470 EN 50524-471, EN 50524-472 EN 50524-473, EN 50524-474 EN 50524-475, EN 50524-476 EN 50524-477, EN 50524-478 EN 50524-479, EN 50524-480 EN 50524-481, EN 50524-482 EN 50524-483, EN 50524-484 EN 50524-485, EN 50524-486 EN 50524-487, EN 50524-488 EN 50524-489, EN 50524-490 EN 50524-491, EN 50524-492 EN 50524-493, EN 50524-494 EN 50524-495, EN 50524-496 EN 50524-497, EN 50524-498 EN 50524-499, EN 50524-500 EN 50524-501, EN 50524-502 EN 50524-503, EN 50524-504 EN 50524-505, EN 50524-506 EN 50524-507, EN 50524-508 EN 50524-509, EN 50524-510 EN 50524-511, EN 50524-512 EN 50524-513, EN 50524-514 EN 50524-515, EN 50524-516 EN 50524-517, EN 50524-518 EN 50524-519, EN 50524-520 EN 50524-521, EN 50524-522 EN 50524-523, EN 50524-524 EN 50524-525, EN 50524-526 EN 50524-527, EN 50524-528 EN 50524-529, EN 50524-530 EN 50524-531, EN 50524-532 EN 50524-533, EN 50524-534 EN 50524-535, EN 50524-536 EN 50524-537, EN 50524-538 EN 50524-539, EN 50524-540 EN 50524-541, EN 50524-542 EN 50524-543, EN 50524-544 EN 50524-545, EN 50524-546 EN 50524-547, EN 50524-548 EN 50524-549, EN 50524-550 EN 50524-551, EN 50524-552 EN 50524-553, EN 50524-554 EN 50524-555, EN 50524-556 EN 50524-557, EN 50524-558 EN 50524-559, EN 50524-560 EN 50524-561, EN 50524-562 EN 50524-563, EN 50524-564 EN 50524-565, EN 50524-566 EN 50524-567, EN 50524-568 EN 50524-569, EN 50524-570 EN 50524-571, EN 50524-572 EN 50524-573, EN 50524-574 EN 50524-575, EN 50524-576 EN 50524-577, EN 50524-578 EN 50524-579, EN 50524-580 EN 50524-581, EN 50524-582 EN 50524-583, EN 50524-584 EN 50524-585, EN 50524-586 EN 50524-587, EN 50524-588 EN 50524-589, EN 50524-590 EN 50524-591, EN 50524-592 EN 50524-593, EN 50524-594 EN 50524-595, EN 50524-596 EN 50524-597, EN 50524-598 EN 50524-599, EN 50524-600 EN 50524-601, EN 50524-602 EN 50524-603, EN 50524-604 EN 50524-605, EN 50524-606 EN 50524-607, EN 50524-608 EN 50524-609, EN 50524-610 EN 50524-611, EN 50524-612 EN 50524-613, EN 50524-614 EN 50524-615, EN 50524-616 EN 50524-617, EN 50524-618 EN 50524-619, EN 50524-620 EN 50524-621, EN 50524-622 EN 50524-623, EN 50524-624 EN 50524-625, EN 50524-626 EN 50524-627, EN 50524-628 EN 50524-629, EN 50524-630 EN 50524-631, EN 50524-632 EN 50524-633, EN 50524-634 EN 50524-635, EN 50524-636 EN 50524-637, EN 50524-638 EN 50524-639, EN 50524-640 EN 50524-641, EN 50524-642 EN 50524-643, EN 50524-644 EN 50524-645, EN 50524-646 EN 50524-647, EN 50524-648 EN 50524-649, EN 50524-650 EN 50524-651, EN 50524-652 EN 50524-653, EN 50524-654 EN 50524-655, EN 50524-656 EN 50524-657, EN 50524-658 EN 50524-659, EN 50524-660 EN 50524-661, EN 50524-662 EN 50524-663, EN 50524-664 EN 50524-665, EN 50524-666 EN 50524-667, EN 50524-668 EN 50524-669, EN 50524-670 EN 50524-671, EN 50524-672 EN 50524-673, EN 50524-674 EN 50524-675, EN 50524-676 EN 50524-677, EN 50524-678 EN 50524-679, EN 50524-680 EN 50524-681, EN 50524-682 EN 50524-683, EN 50524-684 EN 50524-685, EN 50524-686 EN 50524-687, EN 50524-688 EN 50524-689, EN 50524-690 EN 50524-691, EN 50524-692 EN 50524-693, EN 50524-694 EN 50524-695, EN 50524-696 EN 50524-697, EN 50524-698 EN 50524-699, EN 50524-700 EN 50524-701, EN 50524-702 EN 50524-703, EN 50524-704 EN 50524-705, EN 50524-706 EN 50524-707, EN 50524-708 EN 50524-709, EN 50524-710 EN 50524-711, EN 50524-712 EN 50524-713, EN 50524-714 EN 50524-715, EN 50524-716 EN 50524-717, EN 50524-718 EN 50524-719, EN 50524-720 EN 50524-721, EN 50524-722 EN 50524-723, EN 50524-724 EN 50524-725, EN 50524-726 EN 50524-727, EN 50524-728 EN 50524-729, EN 50524-730 EN 50524-731, EN 50524-732 EN 50524-733, EN 50524-734 EN 50524-735, EN 50524-736 EN 50524-737, EN 50524-738 EN 50524-739, EN 50524-740 EN 50524-741, EN 50524-742 EN 50524-743, EN 50524-744 EN 50524-745, EN 50524-746 EN 50524-747, EN 50524-748 EN 50524-749, EN 50524-750 EN 50524-751, EN 50524-752 EN 50524-753, EN 50524-754 EN 50524-755, EN 50524-756 EN 50524-757, EN 50524-758 EN 50524-759, EN 50524-760 EN 50524-761, EN 50524-762 EN 50524-763, EN 50524-764 EN 50524-765, EN 50524-766 EN 50524-767, EN 50524-768 EN 50524-769, EN 50524-770 EN 50524-771, EN 50524-772 EN 50524-773, EN 50524-774 EN 50524-775, EN 50524-776 EN 50524-777, EN 50524-778 EN 50524-779, EN 50524-780 EN 50524-781, EN 50524-782 EN 50524-783, EN 50524-784 EN 50524-785, EN 50524-786 EN 50524-787, EN 50524-788 EN 50524-789, EN 50524-790 EN 50524-791, EN 50524-792 EN 50524-793, EN 50524-794 EN 50524-795, EN 50524-796 EN 50524-797, EN 50524-798 EN 50524-799, EN 50524-800 EN 50524-801, EN 50524-802 EN 50524-803, EN 50524-804 EN 50524-805, EN 50524-806 EN 50524-807, EN 50524-808 EN 50524-809, EN 50524-810 EN 50524-811, EN 50524-812 EN 50524-813, EN 50524-814 EN 50524-815, EN 50524-816 EN 50524-817, EN 5052 |

Immunity is a measure of the ability of electronic products to tolerate the influence of electromagnetic phenomena and electrical energy (radiated or conducted) from other electronic products. In Europe, EMC is included in the CE mark, which in turn is included in the EU's harmonization legislation.

The standards listed below define limits and test methods for electromagnetic emissions and immunity tests. As there is not one test that covers compliance globally, there can be different codes for different regions or applications.

2.1.1 Information Technology Equipment (ITE) standards

These standards apply to multimedia equipment (MME) that has an AC or DC supply voltage not exceeding 600 V. Multimedia equipment (MME) is defined as Information technology equipment (ITE), audio equipment, video equipment, broadcast receiver equipment, and entertainment lighting control equipment.

- EN 55032 Class A: emission standard (commercial, industrial, business), harmonized with international standards
- EN 55032 Class B: emission standard (residential), harmonized with international standards
- EN 55035: immunity standard, harmonized with international standards

2.1.2 Harmonized standards by country/region

- EN 61000-6-1 and EN 61000-6-2: generic standards for compliance (Europe)
- FCC Part 15 Subpart B Class A and B: FCC stipulates rules and regulations for telecommunication devices, referring to emission, not immunity (United States)
- ICES-3(A and B)/NMB-3(A and B) (Canada)
- VCCI Class A and B (Japan)
- KS C 9832 Class A and B, KS C 9835, KS C 9547, KS C 9815 (Korea)
- RCM AS/NZS CISPR 32 Class A and B (Australia/New Zealand)

2.1.3 Additional standards by application/product

- EN 50121-4, IEC 62236-4: provides performance criteria for signaling and telecommunications apparatus which may interfere with other apparatus in the railway environment
- EN 50130-4: applies to the components of alarm systems, including access control systems, CCTV systems, fire detection and fire alarm systems, hold-up alarm systems, intruder alarm systems, social alarm systems

2.2 Safety

- The Low Voltage Directive (2014/35/EU): provides broad objectives for the safety of electrical equipment. Ensures products are safe to use without risk of personal injury or property damage.
- IEC/EN/UL 62368-1: compliance of network cameras, encoders, power supplies to requirements intended to reduce risks of fire, electric shock or injury for anyone who might come into contact with the equipment
- IEC/EN/UL 60950-22: specific safety requirements for outdoor products and outdoor enclosures

- IEC/EN 62471-1: photobiological safety of lamps and lamp systems requirements for exposure limits, prevents hazard to eyes and skin
- EN/UL/CSA 60065: applies to electronic apparatus designed to be fed from the mains, from a supply apparatus, from batteries or from remote power feeding and intended for reception, generation, recording or reproduction respectively of audio, video and associated signals
- IS 13252: India specific compliance of network cameras, encoders, power supplies to requirements intended to reduce risks of fire, electric shock or injury for anyone who might come into contact with the equipment

2.3 Environment

2.3.1 IP rating

The IEC (International Electrotechnical Commission) standard IEC 60529 defines IP (ingress protection or international protection) ratings as a two-digit code. The code defines the level of protection of electrical appliances against the intrusion of solid objects or dust, accidental contact, and water.

Table 2.1 IP ratings - the first digit after IP: foreign solid objects

| Level | Protected against | Effective against |
|-------|-----------------------------|---|
| 0 | Not protected | No protection |
| 1 | Objects larger than 50 mm | Large surface of the body such as back of the hand, but no protection against deliberate contact with a body part. |
| 2 | Objects larger than 12.5 mm | Fingers or other objects can penetrate as far as 80 mm assuming it is safe from hazardous parts. Objects with a diameter of 12.5 mm cannot penetrate fully. |
| 3 | Objects larger than 2.5 mm | Objects, such as tools and thick wires, cannot penetrate at all. |
| 4 | Objects larger than 1 mm | Objects, such as wires and screws, cannot penetrate at all. |
| 5 | Dust protected | Ingress of dust is not completely prevented, but dust does not enter in sufficient quantity to interfere with satisfactory operation of the equipment. |
| 6 | Dust tight | No ingress of dust. |

Table 2.2 IP ratings - the second digit after IP: liquids

| Level | Protected against | Effective against |
|-------|--------------------------------------|---|
| 0 | Not protected | No special protection |
| 1 | Dripping water | Dripping water (vertically falling drops) has no harmful effect. |
| 2 | Dripping water when tilted up to 15° | Vertically dropping water has no harmful effect when the enclosure is tilted at any angle up to 15° from its normal position. |
| 3 | Spraying water | Water falling as spray at an angle up to 60° from the vertical has no harmful effect. |
| 4 | Splashing water | Water splashed against the enclosure from any direction has no harmful effect. |

Table 2.2. IP ratings - the second digit after IP: liquids (Continued)

| | | |
|---|---|---|
| 5 | Water jets | Water projected from a nozzle against the enclosure from any direction has no harmful effect. |
| 6 | Powerful water jets | Water from heavy seas or water projected in powerful jets cannot enter the enclosure in harmful quantities. |
| 7 | Brief immersion in water | Ingress of water in a harmful quantity cannot be possible when the enclosure is immersed in water under defined conditions of pressure and time. |
| 8 | Continuous submersion in water | The equipment is suitable for continuous submersion in water under conditions that shall be specified by the manufacturer. The conditions must be harsher than for IPX7 (see previous). |
| 9 | Water from high pressure and steam jet cleaning | Water directed at the housing from any angle under very high pressure has no harmful effect. |

2.3.2 Other relevant IEC standards

- IEC 60068-2: a standard for environmental testing of electronic equipment and products to assess their ability to perform under environmental conditions including extreme cold and dry heat. The procedures below in this standard are typically intended for objects that achieve temperature stability during the test procedure.
 - IEC 60068-2-1: cold
 - IEC 60068-2-2: dry heat
 - IEC 60068-2-6: vibration (continuous)
 - IEC 60068-2-14: change of temperature
 - IEC 60068-2-27: shock
 - IEC 60068-2-30: damp heat (cyclic)
 - IEC 60068-2-64: vibration (broadband random)
 - IEC 60068-2-78: damp heat (steady state)
- IEC 60825 Class I: a standard for ensuring that the kind of laser used in the laser focus module is safe under all conditions of normal use.

2.3.3 NEMA rating

NEMA (National Electrical Manufacturers Association) is a U.S. based association that provides standards for electrical equipment enclosures. NEMA has launched their own standard NEMA 250 worldwide. NEMA has also adopted and published a harmonizing IP standard, ANSI/IEC 60529, through the American National Standards Institute (ANSI).

NEMA 250 addresses ingress protection, but also considers other factors such as corrosion resistance, performance, and construction details. Because of this, NEMA type is comparable to IP, but IP is not comparable to NEMA.

UL standards UL 50 and UL 50E are based on the NEMA 250 standards. NEMA allows self-certification, while UL enforces compliance by demanding that products pass third-party testing and inspection.

Table 2.3 NEMA ratings for enclosures in non-hazardous locations

| NEMA | Equivalent IP rating | Indoor | Outdoor | Protected against |
|----------|----------------------|--------|---------|---|
| Type 1 | IP10 | X | | Access to hazardous parts and ingress of solid foreign objects (falling dirt). No protection against liquids. |
| Type 3 | IP54 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow). Will be undamaged by the external formation of ice on the enclosure. |
| Type 3R | IP14 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (rain, sleet, snow). Will be undamaged by the external formation of ice on the enclosure. |
| Type 3S | IP54 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow). The external mechanisms remain operable when ice laden. |
| Type 4 | IP56 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow, splashing water, and hosedirected water). Will be undamaged by the external formation of ice on the enclosure. |
| NEMA 4X | IP56 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt and windblown dust). Ingress of water (rain, sleet, snow, splashing water, and hosedirected water). Provides an additional level of protection against corrosion. Will be undamaged by the external formation of ice on the enclosure. |
| Type 6 | IP67 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (hose-directed water and the entry of water during occasional temporary submersion at a limited depth). Will be undamaged by the external formation of ice on the enclosure. |
| Type 6P | IP67 | X | X | Access to hazardous parts and ingress of solid foreign objects (falling dirt). Ingress of water (hose-directed water and the entry of water during prolonged submersion at a limited depth). Provides an additional level of protection against corrosion. Will be undamaged by the external formation of ice on the enclosure. |
| Type 12 | IP52 | X | | Without knockouts. Access to hazardous parts and ingress of solid foreign objects (falling dirt and circulating dust, lint, fibers, and flings). Ingress of water (dripping and light splashing). |
| Type 12K | IP52 | X | | With knockouts. Access to hazardous parts and ingress of solid foreign objects (falling dirt and circulating dust, lint, fibers, and flings). Ingress of water (dripping and light splashing). |
| Type 13 | IP54 | X | | Access to hazardous parts and ingress of sold foreign objects (falling dirt and circulating dust, lint, fibers, and flings.) Ingress of water (dripping and light splashing). Spraying, splashing, and seepage of oil and noncorrosive coolants. |

NEMA TS 2 is a design guide that applies to traffic signaling equipment.

2.3.4 IK rating

IK ratings can be found in IEC/EN 62262, an international standard that specifies degrees of protection against external mechanical impact. Originally approved in 1994 as European standard EN 50102, it was adopted as an international standard in 2002.

Many manufacturers choose to test the weakest part of a product to ensure robustness through the product lifespan.

| Level | IK01 | IK02 | IK03 | IK04 | IK05 | IK06 | IK07 | IK08 | IK09 | IK10 | IK10+* |
|-----------------------|------|------|------|------|------|------|------|------|------|------|--------|
| Impact energy (Joule) | 0.14 | 0.2 | 0.35 | 0.5 | 0.7 | 1 | 2 | 5 | 10 | 20 | 50* |
| Mass (kg) | <0.2 | <0.2 | 0.2 | 0.2 | 0.2 | 0.5 | 0.5 | 1.7 | 5 | 5 | |
| Drop height (mm) | 56 | 80 | 140 | 200 | 280 | 400 | 400 | 300 | 200 | 400 | |

*Impact up to 50 J. Manufacturer must indicate energy, mass, and drop height of striking element.

2.4 Other approvals

2.4.1 Explosion protection

- IEC/EN/UL/SANS/CSA 60079-0: general requirements for construction, testing and marking of Ex equipment and Ex components intended for use in explosive atmospheres.
- IEC/EN/UL/SANS/CSA 60079-1: specific requirements for the construction and testing of electrical equipment with the type of protection flameproof enclosure "d", intended for use in explosive gas atmospheres.

2.4.2 Approvals for midspans

For the cases where a midspan is included with the product, approvals specifically relating to the midspan are listed in this section of the datasheet. Explanations can be found in the previous sections of the current document.

2.4.3 Security in access control

- UL 294: defines requirements regarding construction, performance, and operation of access control systems.

3 Certifications

When a camera is installed in a potentially explosive environment, the housing must meet very specific safety standards. They should protect the environment from potential igniters from the camera and other equipment.

European products must comply with the ATEX directive, and the corresponding international standard is IECEx. North America mainly uses the Class/Division ratings by NFPA70 (National Electric Code, NEC) and CSA C22.1 (Canadian Electric Code, CEC) over the Zone system described in ATEX and IECEx.

Table 3.1 Explosion protection ratings

| Class / Division | Atmos- phere | Definition | Zone (IECEx and ATEX) |
|--------------------------|-----------------|--|--------------------------|
| Class I / Division 1 | Gas | Area in which explosive mixture is continuously present or present for long periods. | Zone 0 |
| Class I / Division 1 | Gas | Area in which an explosive mixture is likely to occur in normal operation. | Zone 1 |
| Class I / Division 2 | Gas | Area in which an explosive mixture is not likely to occur in normal operation and if it occurs, will exist only for a short time. | Zone 2 |
| Class II / Division 1 | Dust | Area in which explosive mixture is continuously present or present for long periods. | Zone 20 |
| Class II / Division 1 | Dust | Area in which an explosive mixture is likely to occur in normal operation. | Zone 21 |
| Class II / Division 2 | Dust | Area in which an explosive mixture is not likely to occur in normal operation and if it occurs, it will exist only for a short time. | Zone 22 |

4 Power

4.1 Power over Ethernet (PoE) classes

PoE classes ensure efficient power distribution by specifying the amount of power that a powered device (PD) will require.

Table 4.1 PoE classes

| Class | Type | Guaranteed power level at Power Sourcing Equipment (PSE) | Maximum power level used by Powered Device (PD) |
|-------|------------------|--|---|
| 0 | Type 1, 802.3af | 15.4 W | 0.44 W - 12.95 W |
| 1 | Type 1, 802.3af | 40.0 W | 0.44 W - 3.84 W |
| 2 | Type 1, 802.3af | 7.0 W | 3.84 W - 6.49 W |
| 3 | Type 1, 802.3af | 15.4 W | 6.49 W - 12.95 W |
| 4 | Type 2, 802.3at* | 30 W | 12.95 W - 25.5 W |
| 6 | Type 3, 802.3bt | 60 W | 51 W |
| 8 | Type 3, 802.3bt | 100 W | 71.3 W |

*This type is also referred to as PoE+.

5 Network

5.1 Protection and security control

There are several ways to counter threats to system assets. Some threats pose risks to devices while others pose risks to networks or data in transit/storage. A few selected security controls that can be applied to devices and networks:

- Credentials (user/password) protect unauthorized access to video and prevent unauthorized access to device configuration. Having different account privilege levels provides control of who has access to what.
- IP address filtering (firewall) reduces the local network exposure of a device and thereby protects it from being accessible to unauthorized clients. This reduces risks in case a device password is compromised and it also mitigates risks in case a new critical vulnerability is discovered.
- IEEE 802.1x: protects the network from unauthorized clients. 802.1x is a network infrastructure protection, using managed switches and RADIUS server. The 802.1x client in the device provides authentication to the device on the network.
- HTTPS (Hypertext transfer protocol secure): protects data (video) from network eavesdropping. The use of signed certificates in HTTPS provides a way for a video client to detect whether it is accessing a legitimate camera or a malicious computer impersonating a camera.
- Signed firmware: is implemented by the software vendor signing the firmware image with a private key, which is secret. When firmware has this signature attached to it, a device will validate the firmware before accepting and installing it. If the device detects that the firmware integrity is compromised, it will reject the firmware upgrade. Axis signed firmware is based on the industry-accepted RSA public-key encryption method.
- Secure boot: a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on signed firmware, secure boot ensures that a device can boot only with authorized firmware. Secure boot guarantees that the Axis device is completely clean from possible malware after resetting to factory default.
- TPM: A trusted platform module is a component that provides a set of cryptographic features suitable for protecting information from unauthorized access. The private key is stored in the TPM and never leaves the TPM. All cryptographic operations requiring the use of the private key are sent to the TPM to be processed. This ensures that the secret part of the certificate remains safe even in the event of a security breach.
- Axis Edge Vault: a secure cryptogenic compute module (secure module or secure element) in which the Axis device ID is securely and permanently installed and stored.

For access to more cybersecurity resources, see axis.com/cybersecurity

5.2 Supported protocols

Many protocols come into play when data is transferred securely from one networked device to another.

5.2.1 Protocol reference models

The best way to understand how the different protocols interact is to examine the Open Systems Interconnection (OSI) communication model. There is also the TCP/IP reference model.

5.2.1.1 OSI reference model

A model that describes data communication between open systems. To provide a service, each layer utilizes the services of the layer immediately below it. Each layer must follow certain rules, or protocols, to perform services.

Layer 7 – Application

Makes functions such as web, file, and email transfer available to applications.

Actual applications, such as web browsers or email programs, exist above this layer and are not covered by the OSI model.

Layer 6 – Presentation (Data)

Ensures that data sent by the application layer of a system can be read by the application layer of another system. Converts system-dependent data formats, such as ASCII, into an independent format, permitting syntactically correct data exchange between different systems.

Layer 5 – Session (Persistent connection between peer hosts)

Provides an application-oriented service and takes care of the process communication between two systems. Process communication begins with the establishment of a session, which provides the basis for a virtual connection between two systems.

Layer 4 – Transport (End-to-end transport (connection-oriented protocol))

Provides reliable data transfer service (through flow control and error control) to Layer 5 and above.

Layer 3 – Network (Packet (addressing/fragmentation))

Performs the actual data transfer, by routing and forwarding data packets between systems. Creates and administrates routing tables and provides options for communicating beyond network boundaries. Data in this layer are assigned destination and source addresses, which are used as the basis for targeted routing.

Layer 2 – Data Link (Frames)

Provides data transmission and controls access to the transmission medium, by combining data into units known as frames. Layer 2 is divided into two sublayers, upper range corresponding to Logical Link Control (LLC) and the lower part corresponding to the media access control (MAC). LLC simplifies data exchange, while MAC controls access to the transmission medium.

Layer 1 – Physical (Bits)

Provides services that support the transmission of data as a bitstream over a medium, such as a wired or wireless transmission link.

5.2.1.2 Transmission Control Protocol/Internet Protocol Reference Model

TCP/IP reference model is another model used to understand protocols and how communication takes place. The TCP/IP reference model falls into four different layers which correspond to the OSI reference model as below.

Table 5.1 Reference models comparison

| OSI model | TCP/IP model |
|------------------------|-----------------------------|
| Layer 7 – Application | Layer 4 – Application |
| Layer 6 – Presentation | |
| Layer 5 – Session | |
| Layer 4 – Transport | Layer 3 – Transport |
| Layer 3 – Network | Layer 2 – Internetwork |
| Layer 2 – Data Link | Layer 1 – Network Interface |
| Layer 1 – Physical | |

5.2.2 Application layer protocols

- **CIFS/SMB** (Common Internet File System/Server Message Block): mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.
- **DDNS** (Dynamic Domain Name System): is used to keep track of a domain name's link to changing IPv4 addresses.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol): automatic assignment and management of IP addresses.
- **DNS/DNSv6** (Domain Name System): converts domain names into their associated IP address.
- **FTP** (File Transfer Protocol): primarily used to transmit files from a server to a client (download) or from a client to a server (upload). Can also be used to create and select directories and rename or delete directories and files.
- **HTTP** (Hypertext Transfer Protocol): primarily used to load text and images from a website to web browser. Network video systems provide an HTTP server service that permits access to the systems through web browsers, for downloading configurations or live images.
- **HTTP/2**: a major revision to the HTTP protocol defined in RFC 7540 and released in February 2015.
- **HTTPS** (HTTP Secure): an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS).
- **MQTT** (Message Queuing Telemetry Transport): a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth.
- **NTP** (Network Time Protocol): used to synchronize the time of a computer client or server to another server.
- **RTP** (Real-Time Transport Protocol): permits the transfer of real-time data between system endpoints.
- **RTCP** (Real-Time Control Protocol): provides out-of-band statistics and control information for an RTP session. It partners with RTP in the delivery and packaging of multimedia data but does not transport any media data itself.
- **RTSP** (Real-Time Streaming Protocol): extended control over the transmission of real-time media.

- **SFTP (Secure File Transfer Protocol):** provides file access, file transfer, and file management over any reliable data stream.
- **SIP (Session Initiation Protocol):** communication protocol for signaling and controlling multi-media communications sessions.
- **SIPS (Session Initiation Protocol Secure):** encrypted version of SIP.
- **SMTP (Simple Mail Transfer Protocol):** the standard for transferring email over the internet. Network cameras support SMTP to allow the sending of email alerts.
- **SNMPv1/v2/v3 (Simple Network Management Protocol):** used to remotely monitor and manage networked equipment such as switches, routers, and network cameras. SNMP support allows network cameras to be managed by open source tools.
- **SOCKS:** permits the transfer of network packets between clients and servers through a remote network proxy.
- **SRTP (Secure Real-Time Transport Protocol):** permits encrypted transfer of real-time data between system endpoints, and is therefore a secure variant of RTP.
- **SSH (Secure Shell):** permits management and debug access to network devices securely over an unsecured network.
- **TLSv1.2/v1.3 (Transport Layer Security):** negotiates a private, reliable connection between the client and the server.

5.2.3 Transport layer protocols

- **TCP (Transmission Control Protocol):** connection-oriented, reliable, and in-order delivery of data streams. Most common protocol for data transport.
- **UDP (User Datagram Protocol):** connectionless transmission service, favors timely delivery of data over reliability.
- **ICMP (Internet Control Message Protocol):** send error messages and operational information indicating that a requested service is not available or that a host or router could not be reached.

5.2.4 Network layer protocols

- **IGMPv1/v2/v3 (Internet Group Management Protocol):** used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships, allows more efficient use of resources when supporting these types of applications.
- **IPv4/IPv6 (Internet Protocol):** an individual public address necessary for internet-enabled devices to communicate. IPv4 is the original version, and it uses 32-bit addresses. IPv6 is the most recent version, and it uses 128-bit addresses that are divided into eight groups of four hexadecimal digits.
- **USGv6:** a technical standards profile for IPv6 defined by the US Government to ensure compatibility when procuring IPv6 enabled network devices.

5.2.5 Data Link layer protocols

- **ARP (Address Resolution Protocol):** is used to discover the MAC address of the destination host.
- **CDP (Cisco Discovery Protocol):** proprietary Cisco protocol used as an alternative to LLDP for discovering information about connected hardware devices.

- **IEEE 802.3 (i, u, ab):** standards for Ethernet defining 10Mb/s (10Base-T), 100Mb/s (100Base-TX), and 1Gb/s (1000Base-T) data communication over twisted pair cabling.
- **LLDP (Link Layer Discovery Protocol):** used in to advertise a device's identity and abilities, as well as other devices connected within the same network.

5.2.6 Discovery protocols

- **mDNS (Bonjour):** can be used to discover network video products using Mac computers, or as a discovery protocol for new devices in any network.
- **UPnP (Universal Plug and Play):** Microsoft operating systems can automatically detect resources (Axis device) on a network.
- **Zeroconf:** automatically allocates a network device to an unused IP address from the range of 169.254.1.0 to 169.254.254.255.

5.2.7 Quality of Service

In an IP network it is necessary to control how network resources are shared to fulfill the requirements of each service.

- **QoS (Quality of Service):** ability to prioritize network traffic so that critical flows can be served before flows with less priority. Greater reliability in a network by controlling the amount of bandwidth an application can use and providing the ability to control bandwidth competition between applications.
- **DiffServ :** network tries to deliver a specific service based on the QoS specified by each packet.

5.2.8 Data transmission methods

There are three different methods for transmitting data on a computer network.

- **Unicast:** most common, sender and recipient communicate on a point-to-point basis. Data packers are sent only to one recipient, and no other clients will receive that information.
- **Multicast:** communication between a single sender and multiple receivers on a network. Reduces network traffic by delivering a single stream of information to many recipients.
- **Broadcast:** sender sends the same information to all other servers on a network, all hosts on the network receive the message and will process it to some extent.

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, intercom and audio systems. Axis has more than 3,800 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website axis.com.