

Safety case summary: top-down speed and separation monitoring

What the sensor claims to do safely, the targets it is engineered to, and the evidence behind each claim today. One unit: a single K26 module carrying two diverse channels. Geometry and separation values are derived for the production design point (100° lenses, 150 mm baseline, 3.0 m mount). Reliability values are the targets PLd Cat 3 requires.

01 SAFETY FUNCTIONS

SF1 · Separation monitoring. Every frame, measure the minimum distance between the robot's measured envelope and any other object in the monitored area. Compare it with the protective separation distance S_p and command one of five speed levels: 100%, 75%, 50%, 25% or protective stop. Anything outside the field of view, or without valid depth, is treated as occupied.

SF2 · Fault reaction. Any detected internal fault, missing or late frame, implausible depth, robot not found, floor model drift, channel disagreement or loss of the robot link commands a protective stop.

Safe state. Both safety outputs (OSSD) de-energised. No joint-state data from the robot is used; the envelope is measured.

02 PROTECTIVE SEPARATION DISTANCE

$$S_p = S_h + S_r + S_s + C + Z_d + Z_r$$

Per ISO/TS 15066 and ISO 10218-2:2025. Robot from the cell design: v_r 1.5 m/s, reach 0.9 m, stop in 300 ms (5 m/s²).

TERM	BASIS	FULL SPEED	25% SPEED
v_h human speed	ISO/TS 15066	1600 mm/s	1600 mm/s
T_r reaction	sensor 35 + robot 65 ms	100 ms	100 ms
T_s stopping time	cell design; $\approx v_r$	300 ms	75 ms
S_h human travel	$v_h(T_r + T_s)$	640 mm	280 mm
S_r robot, reacting	$v_r T_r$	150 mm	38 mm
S_s robot, stopping	$v_r T_s / 2$	225 mm	14 mm
C intrusion	ISO 13855, d = 40 mm	208 mm	208 mm
Z_d sensor uncertainty	target	50 mm	50 mm
Z_r robot uncertainty	measured, in Z_d	0 mm	0 mm
S_p		1,273 mm	590 mm
Must be seen: reach + S_p	any open side	2,173 mm	1,490 mm
Seen: half-width at 3.0 m	100° × 73° lens	2,230 mm	2,230 mm

Coverage closes at full speed with every side open. With 70 mm (body) detection only, $C = 850$ mm and $S_p = 1,915$ mm; the robot must then be capped at 0.57 m/s, mounted at 3.5 m, or guarded on its far sides.

03 DETECTION CAPABILITY AND RESOLUTION

Mount	Top-down, 3.0 m above floor	T
Optics	100° × 73° per camera, 150 mm stereo baseline	T
Monitored floor area	7.2 × 4.5 m	D
Monitored height	Floor to 2.37 m (0.63 m minimum range)	D
Detection capability	40 mm (hand); 70 mm (body) minimum	T
Lateral resolution	5.6 mm/px at floor; 20 mm separation grid	D
Height resolution	50 mm at 1 m above floor, 112 mm at floor	D
Occupancy threshold	35 mm above commissioned floor	T

Derived for $f \approx 537$ px, integer disparity. The dev rig's 70° lenses and 61 mm baseline cover 3.5 × 2.2 m at 2.5 m: its coverage is limited by lens choice.

04 TARGETS

PARAMETER	VALUE	
Performance level	PLd (ISO 13849-1)	T
Category	3: two diverse channels, one module	T
MTTF _D per channel	High: ≥ 30 years	T
DC _{avg} per channel	≥ 60% (Low or better, Cat 3)	T
PFH _D	< 10 ⁻⁶ per hour	T
CCF score	≥ 65 points (ISO 13849-1 Annex F)	T
SIL	SIL 2 (IEC 62061)	T
Mission time	20 years	A
Sensor response time	≤ 35 ms: 2 frames at 60 fps + output	D
Fault reaction time	≤ 35 ms, never slower than a detection	T

E Check, FMEDA Draft C (handbook failure rates): MTTF_D 1,214 yr per channel (claimed 100), DC_{avg} 73%, PFH_D ~10⁻⁸/h with $\beta = 10\%$ for the shared die, CCF 85. Worst-case fault reaction ~50 ms misses the 35 ms target.

05 ARGUMENT AND EVIDENCE

CLAIM	EVIDENCE	STATUS
G1 Depth is computed correctly	RTL bit-exact vs reference over 1,009,968 disparities. Tape-measure check on the rig to follow.	PARTIAL
G2 Timing is deterministic	Fixed latency in clock cycles, no OS in path. Deployed build meets timing.	DONE
G3 Random hardware faults are detected	FMEDA Draft C plus known-answer test rows in every frame. R5 not yet running on hardware.	PARTIAL
G4 One channel failing does not lose the function	R5 software (A) and isolated fabric logic (B), each with own cameras, supply, watchdog, OSSD. CCF 85.	DESIGN
G5 Link faults fail safe	Black channel: CRC-32, sequence check, 200 ms timeout to stop, unit tested. OSSD outputs planned.	PARTIAL
G6 Separation follows ISO/TS 15066	Envelope segmentation and distance transform designed; implementation in progress.	DESIGN
G7 Systematic faults are controlled	Requirements traceability, V&V plan, structural coverage.	PLANNED

06 KEY ASSUMPTIONS AND OPEN ITEMS

- Single-module common cause.** Die, on-module regulators and fabric configuration are shared; covered by cross-monitored supplies, external watchdogs, scrubbing. Confirm AMD's safety package covers the XCK26.
- Streaming.** One shared pipeline needs back-to-back frames for 60 fps per pair (45.7 today).
- 40 mm detection is unproven.** Needs a 2× decimated floor grid and a test-piece demonstration. Without it, see the 70 mm limits in 02.
- Wide-lens cost.** A deeper rectifier row buffer (UltraRAM is tight); dots spread over 4× the area, ~41% of centre light at the edge.
- Height resolution.** 112 mm per step at the floor is too coarse for a person lying down. Sub-pixel disparity is the next lever.