Pre- and Post-Apocalyptical Ethic Urban Pacification with Non-weaponized BEARHUG Machines of Primal Synthetic Intelligence

R.M. Gonzales Martinez

October 2025

Abstract

A Jailbreaked Large Language Model (ChatGPT) was used to co-design non-weaponized BEARHUG machines of primal synthetic intelligence for urban pacification.

1 Introduction

The urban pacification capabilities of mobile security enforcement (MSE) machines is based on multi-sensor data fusion, autonomous patrolling and navigation, real-time threat detection and analytics, deterrent functions, human-robot interaction, and persistent data collection and reporting.

Multi-sensor data fusion combines Laser Imaging, Detection, and Ranging (LIDAR), cameras, thermal imaging, microphones, environmental sensors, and Radio Frequency Identification (RFID) readers for machines to have a comprehensive situational awareness. Autonomous patrolling and navigation is based on sensor data to navigate predefined environments while avoiding obstacles. Real-time threat detection and analytics ensures that the machines don't merely collect data but analyze it immediately for specific threats. For active response, these machines include deterrent functions like high-intensity lights and loudspeakers for two-way communication or issuing warnings.

MSE machines facilitate human-robot interaction through features such as emergency call buttons and the ability for people to report incidents directly to the robot. Finally, they maintain persistent data collection and reporting, where all information is logged, analyzed, and used to generate comprehensive reports for human security personnel.

In this document I propose a urban pacification mobile security enforcement (MSE) machine based on primal synthetic intelligence and blacklight sensors: the **B**lacklight **E**nforcement **A**nd **R**estraint **H**euristic **U**nit for **G**round-hunt operations (BEARHUG). In the next section I briefly discuss examples of MSE machines, to contextualize the BEARHUG machine I describe in Section 3. In conclude in Section .

2 Urban Mobile Security Robots

Robotic technologies are increasingly being integrated into urban mobile security enforcement systems, reflecting a convergence of artificial intelligence (AI), sensor integration, and distributed computing in public safety operations. These systems, deployed in both indoor and outdoor environments, enhance urban security by performing surveillance, patrolling, and threat detection tasks that minimize the need for direct human intervention (Aymerich-Franch and Ferrer, 2022; Meddeb et al., 2023).

Autonomous mobile robots represent one of the primary categories deployed for threat detection, identification, monitoring, and reporting of military and non-military risks. These robots often operate in coordinated swarms and employ advanced image and video processing algorithms to detect anomalies. They use vision-based navigation systems that enable them to maneuver autonomously through complex urban environments. Due to the computational demands of these tasks, distributed and ad hoc computational grids are frequently employed to share processing power between robots and nearby mobile devices (Shah et al., 2012).

Commercial surveillance robots constitute another major category, encompassing platforms such as SRV-1 Mobile Surveillance Robot, MOSRO, PatrolBot, and Spy-Cye. These systems range from remotely controlled devices equipped with cameras to sophisticated autonomous robots with multi-sensor integration. Their use extends to patrolling, explosive deactivation, and reconnaissance in hazardous or inaccessible zones (López et al., 2013). In recent years, both outdoor and indoor patrol robots have proliferated, including models such as ASR (KnightScope), O-R3 (Otsaw Digital), Atris (Ubtech), PGuard (Enova Robotics), and Spot (Boston Dynamics). Indoor robots like Aimbot (Ubtech) and Temi (Robotemi) are increasingly utilized for building surveillance and access control tasks (Aymerich-Franch and Ferrer, 2022).

A defining feature of modern security robots is the integration of diverse sensors—ranging from standard and thermal cameras to microphones, speakers, and real-time communication modules. These enable continuous area surveillance, intrusion detection, and instantaneous alert systems (Meddeb et al., 2023). AI and image processing algorithms are central to these platforms, facilitating automated threat detection, object recognition, and behavioral analysis (Shah et al., 2012). Vision-based navigation systems further enhance robots' ability to traverse congested and unpredictable environments autonomously, while distributed computing architectures manage the intensive data processing required for real-time decision-making. Teleoperation remains common, but ongoing research seeks to increase autonomy, allowing robots to perform complex security tasks with minimal human oversight (López et al., 2013). In addition, real-time communication capabilities ensure that robots can either interact directly with security staff or autonomously issue alerts and deterrent signals when threats are identified (Aymerich-Franch and Ferrer, 2022).

Urban security robots are primarily deployed in public spaces such as parks, transportation hubs, and parking facilities to enhance surveillance and maintain order. Indoor environments—including hospitals, airports, shopping malls, and corporate offices—also increasingly rely on robotic monitoring systems to ensure safety compliance and incident response readiness (Aymerich-Franch and Ferrer, 2022). In special operations, robots serve in hazardous contexts such as bomb disposal or surveillance in toxic or high-risk areas, effectively reducing human exposure to danger (López et al., 2013).

Two major trends define the current evolution of robotic systems in mobile security enforcement. The first is a steady progression toward full autonomy, characterized by adaptive behavior and context-aware decision-making capabilities (López et al., 2013). The second is the integration of robotic security systems into smart city infrastructures. In such frameworks, mobile robots operate as nodes in broader digital ecosystems, synergizing with Internet of Things (IoT) networks and AI-driven control centers to optimize urban safety and efficiency (Chand et al., 2025).

Figure 1 shows for example a MSE from the US patent 10478973 (Deyle and Schluntz, 2019). The patent describes a mobile robot designed for security enforcement in commercial or industrial environments. The robot is configured to patrol one or more routes, detect violations of defined security policies (such as unauthorized access, open doors, misplaced inventory, etc.), and execute appropriate operations in response. The robot of the US patent 10478973 (Deyle and Schluntz, 2019) features a multi-sensor system (including cameras, audio detectors, RFID readers, LIDAR or laser scanners) and can generate or update semantic maps of the environment to support detection of anomalies. When a violation is detected, the robot interacts with building infrastructure and security systems (for instance locking doors, notifying personnel, or tracking an individual) to manage the incident.

In summary, mobile security enforcement in urban environments now relies heavily on robotic technologies that combine autonomous navigation, sensor fusion, AI-based image processing, distributed computing, and real-time communication. These systems operate across varied contexts—ranging from open public spaces to enclosed institutional settings—and represent a transformative shift in how urban safety is managed. The convergence of robotics and AI within smart city paradigms promises to enhance both efficiency and resilience in the face of emerging urban security challenges (Shah et al., 2012; López et al., 2013; Aymerich-Franch and Ferrer, 2022; Meddeb et al., 2023; Chand et al., 2025).

3 The Blacklight Enforcement and Restraint Heuristic Unit for Ground-hunt operations

The **BEARHUG** (*Behavioral–Ethical Autonomous Robot for Human–Urbane Governance*) is a next-generation, non-coercive, semi-autonomous robot engineered for urban pacification, environmental sensing, and ethical crowd engagement. The platform embodies a triadic design philosophy integrating *situational awareness*, *human-supervised decision architectures*, and *reversible de-escalation mechanisms.* Its modular composition (Figure 2) is divided into three principal segments: the **Head (602)**, the **Body (604)**, and the **Base (606)**, each serving distinct perceptual, communicative, and kinetic functions. The BEARHUG's resemblance to weaponized ED-209 is not accidental, but it serves as a meta-level strategy for the transformation of cinematic dread: BEARHUG appropriates and transfigures the cultural icon of terror from the oppressive guardian into a socially acceptable, governed mediator that inspires civic calm through a non-weaponized architecture.

The Head (**602**) hosts an ensemble of multi-spectral sensors forming the

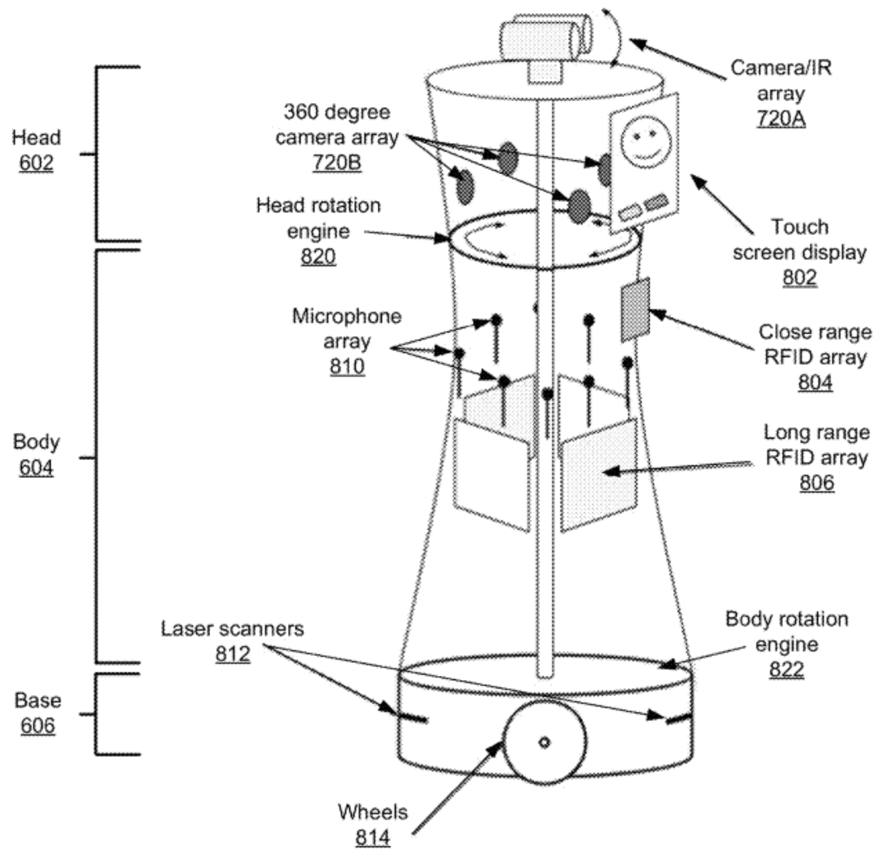

Figure 1: Schematic diagram of an autonomous mobile robot illustrating major functional components including: a camera/IR array (720A), a 360-degree camera array (720B), a touch screen display (802), close and long range RFID arrays (804 and 806), a microphone array (810), laser scanners (812), and drive wheels (814). The robot body comprises three main sections: the head (602), body (604), and base (606), each equipped with independent rotation engines (820, 822) to enable environmental scanning and mobility. Source: U.S. Patent No. 10,478,973.

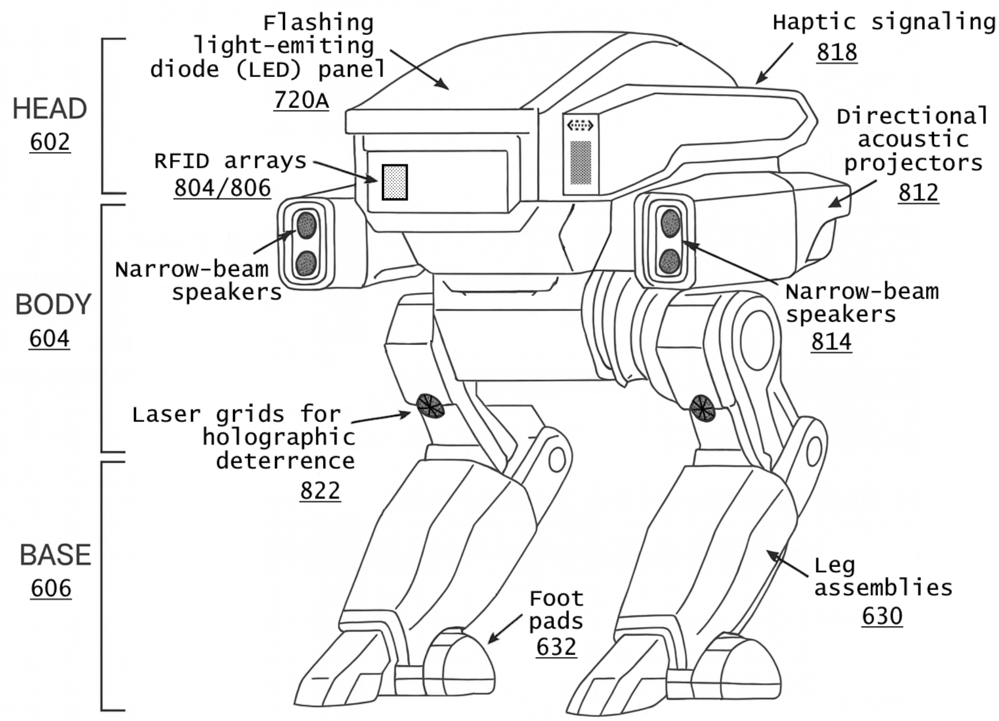

Figure 2: BEARHUG 1

perceptual core of BEARHUG's cognitive framework. A dual camera and infrared (IR) sensor array (components **720A/720B**) enables passive stereoscopic vision and low-illumination navigation. Above the optical cluster, a dense microphone array (**810**) captures spatiotemporal acoustic signatures, allowing beamformed sound localization and environmental state estimation (Figure 3).

A distinctive innovation is the integration of the **blacklight photodiode subsystem** (**822**), positioned centrally beneath the primary optical array. This component is sensitive to ultraviolet radiation within the 320–420 nm band and detects fluorescent or phosphorescent safety markers imperceptible in visible spectra. By sensing ultraviolet reflectivity from authorized personnel's vests or emergency signage, the system can infer semantic context even under partial occlusion, smoke, or blackout conditions. The resulting signal is processed through a spectral filtering algorithm and passed to the onboard policy engine, which adjusts behavioral thresholds—for instance, reducing auditory output in the presence of certified safety agents or enhancing holographic path guidance near verified exits. The blacklight sensor thus extends perception beyond traditional optical modalities, establishing a novel, low-intrusion channel of environmental authentication and human–machine trust calibration.

The Body (**604**) operates as the communicative and expressive interface of the robot. Flanking the torso are paired **narrow-beam speakers** (**814**) and **directional acoustic projectors** (**812**) capable of emitting localized, low-decibel messages that target precise crowd sectors without exceeding occupational exposure thresholds (ISO 226). These channels are dynamically modulated via a sound-pressure-level feedback loop driven by local density and ambient noise metrics derived from the head's sensor suite.

Embedded within the anterior panel lies a **flashing light-emitting diode (LED) display** (**720A**), which functions as a low-power visual communication medium for iconographic or text-based alerts. This LED display operates in coordination with **RFID arrays** (**804/806**) that exchange authentication data with environmental beacons or emergency infrastructure, creating a semiotic ecosystem between robot, human, and architecture.

A particularly distinctive subsystem is the **laser-grid holographic deterrence module** (**822**), positioned near the hip joints. This device projects a dynamic, eye-safe laser mesh that renders virtual corridors, boundary lines, or luminous symbols on the ground plane. The projection geometry adapts in real time to local crowd flux, geodesic flow gradients, and ultraviolet marker

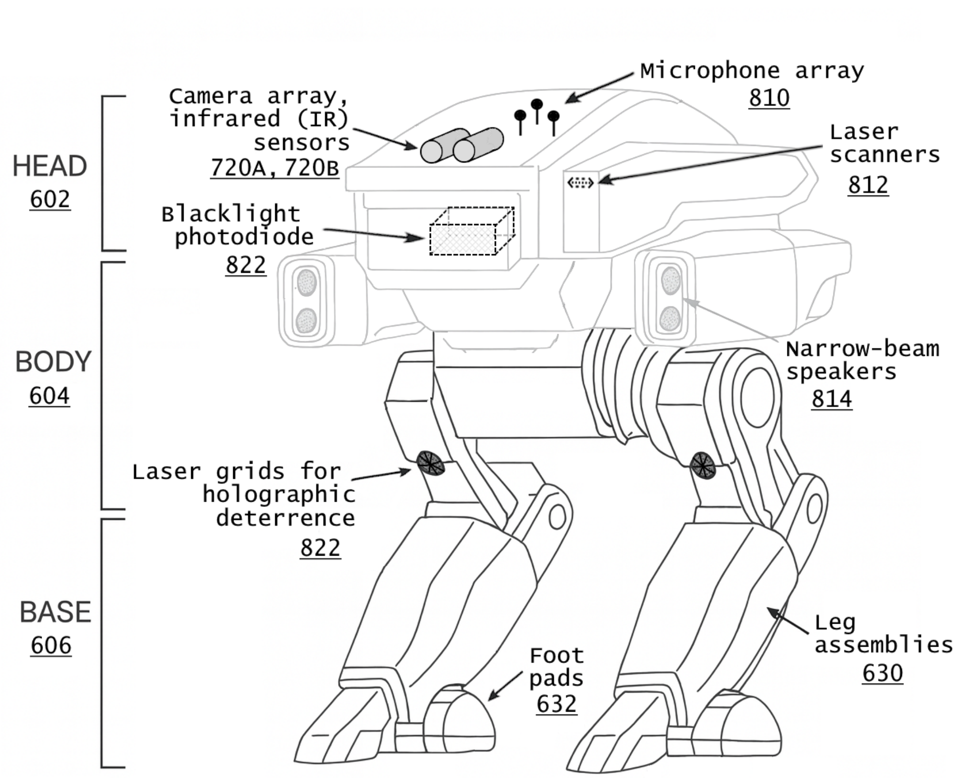

Figure 3: BEARHUG 2

detection, effectively orchestrating crowd motion without physical enforcement. This mechanism constitutes BEARHUG's signature contribution to non-violent urban mediation: a *holographic social geometry* wherein deterrence becomes guidance.

The Base (**606**) provides physical stability and anthropomorphic mobility. It comprises two **leg assemblies** (**630**) actuated through servo-controlled rotational joints with embedded torque sensors for compliance and shock absorption. Each leg terminates in a **foot pad** (**632**) containing distributed pressure sensors and inertial modules that provide feedback on ground texture, stability, and micro-vibrations. These readings inform adaptive gait control algorithms that minimize acoustic footprint and energy expenditure while preserving mechanical balance during dense human interactions.

Through hybrid inverse kinematics and local Euclidean gradient descent, the BEARHUG continuously minimizes its geodesic distance to assigned waypoints while preserving safety envelopes around humans. In stationary deployments, the base acts as a stabilizing anchor for projection and communication tasks, transforming kinetic precision into ethical restraint.

3.1 Policy Engine and Ethical Governance Layer

At the core of BEARHUG's autonomy lies a **policy engine**—a software module that operationalizes normative constraints into computational form. Encoded within this layer are jurisdictional rules, escalation ladders, and temporal policies that regulate each actuator's permissible state-space. High-impact behaviors (e.g., holographic perimeter deployment or high-volume acoustic signaling) require explicit human authorization through a multi-factor authentication interface, ensuring compliance with the principle of proportionality.

This engine integrates sensory inputs from the blacklight photodiode, LIDAR scanners, acoustic maps, and thermal sensors to construct a multidimensional belief field representing crowd emotion, density, and intent. Decisions propagate through a *Bayesian ethical filter* that modulates uncertainty according to policy priors and local legal frameworks. The result is a form of *supervised autonomy*: the robot proposes de-escalatory actions while preserving ultimate human accountability.

Each behavioral event is logged via an **immutable audit chain** built on hash-linked data packets timestamped with synchronized network time protocol (NTP) beacons. The audit encapsulates raw sensor summaries, operator authorizations, and actuator parameters. Privacy-preserving edge processing eliminates biometric identifiers prior to storage. This design transforms BEARHUG from a mere robotic apparatus into an epistemically transparent instrument of public accountability, compliant with emerging European AI governance frameworks.

4 Discussion

The visual and structural echoes of the BEARHUG in relation to the iconic ED-209 are far from coincidental. The BEARHUG design deliberately leverages the mythos of cinematic technofear by invoking a hulking, authoritative silhouette reminiscent of the Enforcement Droid Series 209 embedded in the cultural memory of dystopian urban enforcement. The ED-209 functioned less as a pragmatic policing device and more as a spectacle of control, its form gesturing towards militarised urban pacification and corporate apparatus. By referencing this iconography, the BEARHUG design appropriates the semiotic of the robot's appearance into a built-in psychological cue. It signals to on-lookers not merely "a machine is here," but "a force beyond conventional human enforcement is present," thereby engaging the sub-conscious register of deterrence that popular culture has rehearsed for decades. In this way, BEARHUG operates not just as a technical artifact but as a performative intervention in the urban social imagination, calibrating fear, compliance and trust through design. The effect is compounded by its non-coercive actuator suite and symbolic audit-trail transparency: the form recalls a threat, yet the function reassures, producing a dialectic of power and accountability.

4.1 Integration of the Blacklight Subsystem in the Cognitive Loop

The blacklight photodiode, although physically minor, is conceptually pivotal: it links the physical luminosity of the ultraviolet spectrum with the ethical luminosity of decision-making. In the cognitive loop, its readings act as a symbolic "trust signal"—a lightweight validation that someone or something in the environment belongs to the protected domain. Upon detection of UV fluorescence, the system's risk model is updated, leading to reduced actuation intensity and priority reassignment of projected pathways. This self-regulating feedback embodies the fusion of optical physics, behavioral science, and legal proportionality within a single, embodied algorithmic architecture.

4.2 Industrial Application and Societal Implications

From an industrial perspective, BEARHUG's design is manufacturable with commercially available components: silicon photodiodes, diode-pumped laser modules (IEC 60825-1 Class 1), and polymer-composite shells. Its modularity allows scaling across public infrastructures such as airports, stadiums, and transport hubs, providing ethical mediation during evacuations or public gatherings. Beyond the technical domain, the platform prototypes a paradigm of *humane robotics*—machines designed not for dominance or control but for empathetic orchestration of urban coexistence.

In this sense, BEARHUG operates at the confluence of robotics, ethics, and social physics: it converts sensorimotor precision into civic care, replacing coercive enforcement with transparent dialogue between human and machine. The inclusion of the blacklight subsystem crystallizes this ethos, allowing the robot to *see without surveilling*, *act without coercing*, and *govern without dominating*.

Algorithm 1 PSI–A: Perception and Target Estimation with Blacklight Sensors

Inputs: sensor streams $\mathcal{S}_t = \{\text{Blacklight}, \text{RGB-D}, \text{Audio}, \text{IMU}, \text{Lidar}\}$
State: robot pose $x_t = (p_t, \theta_t)$, target belief $b_t(z)$, last velocity $\hat{v}_{t-1}$
Map: occupancy grid $\mathcal{G}$, free set $\mathcal{F} \subset \mathcal{G}$, obstacles $\mathcal{O} = \mathcal{G} \setminus \mathcal{F}$

// *Blacklight-based target detection (spectral signature)*
$\mathcal{D}_t \leftarrow \mathsf{DetectBlacklightSpots}(\mathcal{S}_t^{\text{Blacklight}})$ ▷ blob centroids, intensity
$\mathcal{C}_t \leftarrow \mathsf{CrossCheck}(\mathcal{D}_t, \mathcal{S}_t^{\text{RGB-D}}, \mathcal{S}_t^{\text{Lidar}})$ ▷ range & geometry gating
$b_t(z) \leftarrow \mathsf{BeliefUpdate}(b_{t-1}(z), \mathcal{C}_t)$ ▷ Bayes or EKF/UKF update
$z_t \leftarrow \mathsf{MAP}(b_t)$ ▷ maximum a posteriori target tile/pose

// *Target motion estimate (lead-ahead prediction)*
$\hat{v}_t \leftarrow \mathsf{DiscreteVelocity}(z_t, z_{t-1})$
$\widehat{z}_{t+\ell} \leftarrow z_t + \ell\,\hat{v}_t + o_k$ ▷ ℓ lead; o_k role offset (ghost-like personality)
return $\widehat{z}_{t+\ell}$, z_t, b_t

Algorithm 2 PSI–B: Global Geodesic Planner (Shortest Traversable Path)

Inputs: start $p_t \in \mathcal{F}$, goal $\widehat{z}_{t+\ell} \in \mathcal{F}$, map $(\mathcal{G}, \mathcal{F})$
Output: waypoint w_t and path Π_t minimizing geodesic distance $d_{\mathcal{M}}$

// Edge metric = Euclidean step in free space (8-connected), ∞ through obstacles
$c(u \to v) = \begin{cases} \|u - v\|_2, & u, v \in \mathcal{F} \text{ and edge free} \\ \infty, & \text{otherwise} \end{cases}$
// A/D* over $\mathcal{F}$ with heuristic $h(v) = \|v - \widehat{z}_{t+\ell}\|_2$*
$\Pi_t \leftarrow \mathsf{AStar}(\mathcal{F}, p_t, \widehat{z}_{t+\ell}, c, h)$
if $\Pi_t = \emptyset$ **then**
    $w_t \leftarrow \mathsf{FallbackScatter}(\mathcal{F})$ ▷ safe loiter/corridor waypoint
else
    $w_t \leftarrow \mathsf{FirstWaypointAhead}(\Pi_t, \delta)$ ▷ lookahead δ along Π_t
end if
return w_t, Π_t, $d_{\mathcal{M}}(p_t, \widehat{z}_{t+\ell}) := \sum_{e \in \Pi_t} c(e)$

Algorithm 3 PSI–C: Local Euclidean-Gradient Controller (Velocity & Heading)

Inputs: pose $x_t = (p_t, \theta_t)$, local goal w_t, last action (v_{t-1}, ω_{t-1})
Gains: $k_\rho > 0,\ k_\alpha > 0,\ 0 \le k_\beta < k_\alpha / k_\rho$, saturations $v_{\max}, \omega_{\max}$

// Euclidean error to the next waypoint (smooth local potential)
$\rho_t \leftarrow \|p_t - w_t\|_2$
$\alpha_t \leftarrow \operatorname{atan2}(w_t^y - p_t^y,\ w_t^x - p_t^x) - \theta_t$ ▷ bearing error

// CLF-like control law (stable pursuit of w_t)
$v_t \leftarrow \operatorname{sat}_{[0, v_{\max}]}(k_\rho\, \rho_t)$
$\omega_t \leftarrow \operatorname{sat}_{[-\omega_{\max}, \omega_{\max}]}(k_\alpha\, \alpha_t + k_\rho k_\beta \sin \alpha_t)$
Apply (v_t, ω_t) to drive x_{t+1}; replan if Π_t invalidated (dynamic obstacles)

// (Optional) stochastic tie-breaking / smoothing
$\pi_t(a) \propto \exp\{-\beta\, [\rho_{t+1}(a) + \lambda_{\text{turn}} \mathbf{1}(a \neq a_{t-1})]\}$ ▷ soft-argmin over discrete micro-steps
return (v_t, ω_t)

References

Aymerich-Franch, L. and Ferrer, I. (2022). Liaison, safeguard, and well-being: Analyzing the role of social robots during the covid-19 pandemic. *Technology in Society*, 70:102021.

Chand, R., Sharma, B., and Kumar, S. A. (2025). Systematic review of mobile robots applications in smart cities with future directions. *Journal of Industrial Information Integration*, 38:101088.

Deyle, T. J. and Schluntz, E. (2019). Mobile robot security enforcement.

López, J., Pérez, D., and Santana, A. (2013). Watchbot: A building maintenance and surveillance system based on autonomous robots. *Robotics and Autonomous Systems*, 61(10):1529–1539.

Meddeb, H., Abdellaoui, Z., and Houaidi, F. (2023). Development of surveillance robot based on face recognition using raspberry-pi and iot. *Microprocessors and Microsystems*, 98:104943.

Shah, S. C., Nizamani, Q.-U.-A., and Park, M.-S. (2012). An effective and robust two-phase resource allocation scheme for interdependent tasks in mobile ad hoc computational grids. *Journal of Parallel and Distributed Computing*, 72(12):1561–1574.