Maciej Urbański

IT PROJECT MANAGER & AI AUTOMATION ENGINEER

Warsaw, Poland (Remote-first) · EN / PL · maciej@theurbanscy.com · +48 793 567 797 · LinkedIn · GitHub · maciej.theurbanscy.com

SUMMARY

I build applied AI systems — **MCP servers, agent loops, retrieval, and evals — with a confirm gate on every write.** Production proof runs via a governed **Wrike MCP** in the system of record. Current build is a **Halo ITSM MCP** over a live service desk: conversation-shaped tools, not a REST wrapper, as the tool layer for a full agentic ticket loop (planner · traces · evals).

CORE COMPETENCIES

Agent systems	**MCP server & tool design** · planner loops · confirm-gated writes · human-in-the-loop
Retrieval & evals	**Agentic / hybrid / graph RAG** · embeddings & chunking · Langfuse traces · tool-use evals
Engineering	**TypeScript · Python · SQL · Zod · APIs** · multi-site identity, POS & workplace systems

TECH STACK

Languages	`TypeScript · Python · SQL · Node.js · PowerShell · Bash`
AI	`MCP (stdio) · agent loops · Zod schemas · RAG (agentic/hybrid/graph) · embeddings · Langfuse · evals`
Platforms	`Bun · Docker · Linux · Halo ITSM · Wrike · Google Workspace · AWS`

SELECTED PROJECTS — AGENT STACK

Wrike MCP — PRODUCTION

`TypeScript · Bun · MCP SDK · Zod · Wrike API`

Conversation-shaped MCP servers governing **live tasks in the system of record**. Narrow mutations (rename, description, status, parents), a YAML item-type registry, and a space-locked variant so changes can't drift across accounts. Ships as stdio **and** streamable HTTP. *A person still accepts the change in Wrike.*

Halo ITSM MCP — LIVE · IN BUILD

`TypeScript · Bun · MCP SDK · Zod · OAuth2`

MCP server over one live Halo instance. Tools match what a technician *says* — prove identity, find a ticket, load it, note it, reply to the store user — not the REST catalog. OAuth2 token cache with refresh; **mutating tools preview and refuse unless `confirm: true`**. Resolve-ticket closes the loop next.

Halo ITSM Agent — LIVE · IN BUILD

`TypeScript · Bun · Zod · MCP · SSE · Langfuse · Tactical RMM`

Agent that **triages tickets, tracks SLAs, and gathers the missing detail** a human agent needs to resolve — plan → execute tools → stream a handoff summary. Calls **Tactical RMM** to run first-step troubleshooting on the endpoint before escalating, then packages findings onto the ticket. Runtime tool registry (native + MCP discovery), Langfuse-wrapped observer, SSE + session-replay JSON, abort / max-steps bounds. **The agent diagnoses and enriches; a human agent resolves.**

AI_devs Framework

`Python · TypeScript · SQLite FTS5 + sqlite-vec · Neo4j · Langfuse`

Agent framework + solved tasks: JSON-schema tool loops, MCP adapter, agentic/hybrid/graph RAG, synthetic tool-use & response-correctness evals, sandboxed code exec (QuickJS/Deno), a separate Whisper transcription MCP.

PDFMD — Secure Document AI

`Python · PyMuPDF · marker-pdf · AES-GCM vault`

One pipeline across CLI, PySide6 GUI, and MCP. **PII scan + anonymize run before any cloud LLM call**; reversible AES-GCM vault; `plan()` is data, `run()` executes.

EXPERIENCE

IT Project Manager & Group Technical Lead — 2016 – Present

Multi-site hospitality & retail ops. Promoted Support Lead → SysAdmin → IT PM / Group Technical Lead. Own the multi-site network (identity, POS/payments, workplace) the agents act in. UAT, go-live, and hypercare decide where a tool is allowed to write.

- **Google Workspace** — zero-downtime identity cutover across multi-site operations; HR-driven provisioning as the standard path
- **Deliverect × POS** — revenue-critical vendor integration through requirements, UAT, go-live, IT/ops ownership
- **Settlement reconciliation** — BLIK vs POS; month-end surprises replaced by near real-time operational alerts
- **Warehouse (lightweight WMS)** — Next.js/React/Prisma/SQLite app live on the floor (mikr.us); catalog, search, photo cards, stock movements, CSV export; password-gated, pm2, hot SQLite backups

CREDENTIALS

AI_devs 4 Builders (Professional) `2026-10-01` verify ↗

AI_devs 3 Agents (Professional) `2025-03-03` verify ↗