Project Cartesian: Technical Audit & Structural Map

Status: Auditing `src/cartesian-core/src/` (Rust Monolith Internals).

1. Directory Structure Map

- `ProjectCartesian/`
  - `docs/` — (Project Documentation & Context PDFs)
  - `iso/` — (ArchISO Configuration & Docker Builder)
    - `archiso_profile/` — (Custom ISO Definitions)
      - `airootfs/` — (Live Filesystem Overlays: etc, home, root)
      - `bootstrap_packages`
      - `packages.x86_64`
      - `pacman.conf`
      - `profiledef.sh`
    - `build.sh` — (The Factory Script)
    - `Dockerfile` — (The Builder Image)
  - `pkg/` — (Distribution Packaging)
    - `cartesian-admin.sh` — (Privilege Bridge)
    - `PKGBUILD` — (Arch Build Recipe)

    - `org.cartesian.policy` — (Polkit Policy)
    - `50-cartesian.rules` — (Polkit Rules)
  - `src/`
    - `cartesian-core/` — (Rust Monolith)
      - `src/` — (main.rs, lobotomy.rs, inference.rs)
      - `Cargo.toml`
      - `main` — (Binary Leakage)
    - `configs/` — (Master DE Templates)
  - `repo/` — (Local Binary Repo - Ignored)
  - `.gitignore`
  - `build_windows.bat`

3. Qualitative Analysis Notes

A. Non-Standard Logic

- **Polkit Bridge:** Argument parsing in `cartesian-admin.sh` is brittle. A malformed PID could potentially lead to shell injection if not carefully sanitized in the Rust caller.
- **Mounting Races:** The `sleep` based mounting in `hyprland.conf` is a "magic number" fix that will eventually fail on slower or heavily loaded host machines.

B. Efficiency Bottlenecks

- **Rust Refresh:** `sysinfo`'s `refresh_processes()` is heavy. On a standard Arch system with 200+ processes, doing this at 1Hz or faster creates a constant CPU floor that competes with the AI and Games.

C. Security Concerns

- **Silent Root Escalation:** The combination of `autologin` + `empty shadow` + `NOPASSWD Polkit` creates a system where a single "hallucination" by the AI could result in non-consensual system-wide changes (e.g., `kill -STOP 1001` where 1001 is the user's browser).

File/Folder	Issue Type	Description	Potential Fix	Priority	Status
shadow	Security	root and cartesian users have empty passwords in airootfs.	Use openssl passwd -6 to generate secure hashes.	Critical	FALSE
autologin.conf	Security	Instant unauthenticated TTY1 access combined with empty passwords.	Implement "User Security Protocol" (hashes).	High	FALSE
50-cartesian.rules	Security	polkit.Result.YES for wheel allows unprompted root access for AI.	Require password for sensitive Polkit actions.	High	FALSE
pacman.conf	Roundabout	Infinite append loop of	Implement "Configuration	High	FALSE

		[cartesian] block in build.sh.	Sanitization Protocol" (marker-based sed).		
build.sh	Security	Python HTTP server binds to 0.0.0.0 (all interfaces).	Bind strictly to 127.0.0.1.	High	FALSE
lobotomy.rs	Inefficient	O(n) process scan via System::new_all() on every UI tick.	Use refresh_processes_specifics or async throttling.	High	FALSE
PKGBUILD	Security	sha256sums set to 'SKIP'.	Use updpkgsums for integrity verification.	High	FALSE
cartesian-admin.sh	Security	Can kill -STOP any PID > 1000, including the compositor.	Implement a specific whitelist of allowlisted process names.	Medium	FALSE
hyprland.conf	Roundabout	Shared folder mount relies on sleep 4 and manual sudo.	Move to /etc/fstab with x-systemd.automount.	Medium	FALSE
src/configs	Roundabout	Duplicates of files in airootfs leading to config drift.	Implement "SSOT Protocol" (symlinks or build-time sync).	Medium	FALSE
config.toml	Inefficient	jobs = 2 hard limit prevents	Use environment	Medium	FALSE

		multi-core build scaling.	variables for dynamic job allocation.		
packages.x86_64	Inefficient	rust and cargo included in final Live ISO (~500MB bloat).	Move to makedepends only.	Medium	FALSE
mkinitcpio.conf	Not Optimal	Hardcoded vbox and virtio drivers in MODULES.	Use autodetect hook or conditional loading.	Medium	FALSE
build.sh	Inefficient	Double-copying packages from pkg/ -> repo/ -> local_repo/.	Use symlinks for the local repository folder.	Medium	FALSE
main.rs	Not Optimal	UI Tick drives monitoring; blocks UI if scan is slow.	Use an async background task for monitoring.	Medium	FALSE
cartesian-core/	Non-Standard	Compiled main binary exists in source root.	Add to .gitignore and delete from source tree.	Medium	FALSE
.bash_profile	Efficiency	dbus-run-session starts a new bus every login.	Use systemd --user session bus.	Medium	FALSE
sudoers	Roundabout	Redundant NOPASSWD for mkdir/mount given wheel membership.	Consolidate logic based on intended security posture.	Low	FALSE
config.toml	Not Optimal	build.linker =	Move to	Low	FALSE

		"gcc" generates unused key warning.	[target.x86_64-unknown-linux-gnu] block.		
.bash_profile	Not Optimal	Manual creation/chmod of XDG_RUNTIME_DIR.	Rely on pam_systemd.	Low	FALSE
profiledef.sh	Non-Standard	iso_version is dynamic (date-based), breaking determinism.	Use static version or git commit hash.	Low	FALSE
waybar_style	Inefficient	Invalid comment syntax (//) in CSS.	Replace with /* ... */.	Low	FALSE
build.sh	Robustness	kill -9 on port 8050 and sleep 2 for server start.	Use nc or curl loop to verify server health.	Low	FALSE
build_windows.bat	Robustness	No existence check for iso/Dockerfile before build.	Add IF EXIST validation.	Low	FALSE
.gitignore	Optimization	Standard Windows files (Thumbs.db) not blocked.	Add generic Windows OS patterns.	Low	FALSE