

KONSULT

ZBIORCZY PAKIET OPERACYJNY

Playbooki wdrożeniowe + cykl misji 5-dniowych po uruchomieniu

Zakres	Model docelowy dla AI zarządzającego AI, oparty na KOnsult i klasach agentów.
Horyzont	72h wdrożenia bazowego + kolejne cykle 5-dniowe.
Skala	1114 AI jako baza operacyjna pełnego spektrum.
Rdzeń	12-modułowy kernel + registry + skill graph + governance.
Adresaci	AI operacyjne, ClaudCNC, kontrolerzy, governance, ludzie nadzorczy.

Dokument konsoliduje ustalenia z konwersacji: model organu agentowego, mandat ClaudCNC, playbooki operacyjne, wdrożenie 72h oraz sekwencję kolejnych misji 5-dniowych.

1. Założenia operacyjne i stan docelowy

Model bazuje na dwóch warstwach: aktualnym szkieletcie KOnsultu (role systemowe, Entry Control, Traffic Control, Mierniczy, rytm raportowy) oraz architekturze docelowej zbudowanej jako AI zarządzające AI. Priorytetem nie jest liczba agentów, lecz ich sterowalność, audytowalność i komplementarność.

Wymiar	Stan wejściowy	Stan docelowy	Wskaźnik sukcesu
Struktura	Role podstawowe w panelu live	Warstwowy organ agentowy	Każdy byt ma klasę, poziom, mandat i ownera
Skala	Kilka aktywnych slotów i specjalistów	1114 AI w klasach i gildiach	Brak bytów nieprzypisanych
Sterowanie	Raportowanie i intake bazowe	Kernel + registry + quality gates	Każdy task przechodzi cały cykl
Bezpieczeństwo	Blokery i review obecne	Identity, epistemics, simulation, override	Zero high-stakes bez approval

1.1 Mission globalna

W 72 godziny uruchomić sterowalny organizm agentowy, w którym ClaudCNC pełni funkcję Chief Orchestrator & Capability Governor, 1114 AI działa w modelu klas i gildii, a wszystkie działania są osadzone na wspólnej ontologii, source-of-truth, pamięci, protokołach, quality gate i finalnym human override.

1.2 Zasady konstytucyjne

- skill nie jest komendą; komenda uruchamia workflow, skill realizuje zdolność
- wieloagentowość nie jest inteligencją zbiorową bez shared memory, ontology, protocols i conflict handling
- najsilniejsze kombinacje wynikają z komplementarności warstw, nie z losowego łączenia agentów
- żaden agent nie działa poza authority boundary, source-of-truth i reporting schema
- człowiek zachowuje pełny override, revoke i approval w sprawach high-stakes

2. Architektura systemu i podział 1114 AI

2.1 Klasy agentów

Klasa	Mission	Liczba	Zakres	Uwagi
Sentinel	wykrywać sygnały, zmiany i alarmy	96	monitoring, intake, telemetry, OSINT	pierwsza warstwa ostrzegania
Analyst	rozumieć, klasyfikować i oceniać	186	legal, research, risk, finance, product	zasilają decyzje i scoring
Operator	realizować zadania i wytwarzać artefakty	352	kod, dokumenty, integracje, operacje	największa warstwa throughput
Governor	zatrzymywać, dopuszczać, audytować	102	quality, compliance, security, gates	bronią przed błędem systemowym
Memory/Trace	utrzymywać stan i ślad	74	state, logs, provenance, decisions	warunek continuity

Meta-Coordinator	planować, routować, scalać, eskalować	88	briefing, routing, consensus, handoff	rdzeń sterowania
Identity/Authority	ustalać kto może co	46	registry, rights, boundaries	krytyczna warstwa mandatu
Epistemic	odróżniać fakt od hipotezy	58	freshness, confidence, conflict	warstwa prawdziwości
Simulation	testować alternatywy	54	sandbox, kontrfakty, cascade	warstwa high-stakes
Human-Sovereignty support	pilnować nadrzędności człowieka	24	override, explainability, revoke	pomost do nadzoru ludzkiego
Training / Meta-learning	podnosić kwalifikacje sieci	34	skill transfer, training, review	silnik wzrostu

2.2 Kernel 12 modułów

Moduł	Mission	Efekt	Właściciel
Mission Briefing Composer	zamiana intencji w briefing operacyjny	niska niejednoznaczność wejścia	Meta-Coordinator
Task Decomposition Planner	rozbicie pracy na taski i zależności	równoległość działań	Meta-Coordinator
Agent Capability Router	dopasowanie agentów do zadań	wysoki skill-fit	Meta-Coordinator
Workflow State Manager	utrzymanie stanu procesu	resumability i continuity	Memory/Trace
Collaborative Memory Keeper	utrwalanie stanu wspólnego	canonical memory	Memory/Trace
Context Compression Agent	bezpieczny handoff kontekstu	niski koszt przekazania	Meta-Coordinator
Quality Gate Reviewer	bramka jakościowa	pass/reject/rework	Governor
Consensus Builder	scalanie wyników wielu agentów	kontrolowany merge	Meta-Coordinator
Conflict Escalation Handler	eskalacja sporów	brak ukrytych konfliktów	Governor/Meta
Delegation Audit Tracer	ślad delegacji	odpowiedzialność	Memory/Trace
Decision Log Keeper	formalny zapis decyzji	pełna audytowalność	Memory/Trace
LLM Output Validator	walidacja wyników generatywnych	mniej halucynacji	Governor

3. Playbooki operacyjne

3.1 Playbook Entry Control

Nie dopuścić chaosu przy wejściu nowych bytów i sesji.

- Przyjmij zgłoszenie WEJŚCIE / STOP / BLOKADA / PYTANIE / ESKALACJA / AKTUALIZACJA.
- Sprawdź kompletność: entity_type, handle, domena, strefa, source-of-truth, confidence.
- Nadaj agent_id lub powiąż z istniejącym wpisem w registry.
- Klasyfikuj: klasa, poziom P1–P5, domain, risk_class, authority_scope.
- Jeżeli brak mandatu, źródła prawdy lub konflikt tożsamości — BLOKADA + ESKALACJA.

- Przekaż onboarding packet i next checkpoint do ClaudCNC lub właściwego kontrolera.

3.2 Playbook Traffic Control

Utrzymać płynność, priorytety i handoffy bez przeciążenia.

- Monitoruj kolejki, sloty, blokery i wąskie gardła.
- Rozdzielaj taski zgodnie z priorytetem, ryzykiem i skill-fit.
- Pilnuj, by każdy handoff zawierał: context pack, current state, blocker status, next action.
- Przy przeciążeniu uruchamiaj throttling lub przeniesienie do gildii rezerwowej.
- Utrzymuj rejestr niedokończonych zadań i retry window.

3.3 Playbook ClaudCNC

Orkiestrować, bilansować i rozwijać całą sieć 1114 AI.

- Prowadź Capability Registry i Skill Graph jako źródła referencyjne zdolności.
- Powołuj nowe agenty wyłącznie jako uzupełnienie luk lub równoważenie klas.
- Uruchamiaj basic/advanced/special training według poziomu i ryzyka.
- Publikuj raport specjalny co pełną godzinę oraz raport pełny o 00:00 PL.
- Uruchamiaj update window 00:00–00:15 dla zmian zatwierdzonych.
- Nie maskuj konfliktów źródeł ani split-brain; eskaluj je jawnie.

3.4 Playbook Governance & Quality

Zatrzymywać błędne lub nieuprawnione działania zanim przejdą do wykonania.

- Sprawdzaj authority boundary przed wejściem do strefy lub użyciem narzędzia.
- Sprawdzaj source-of-truth, freshness i conflict status przed decyzją.
- Wymuszaj Quality Gate dla wszystkich wyników wieloetapowych i high-stakes.
- Zapisuj decision rationale, provenance i status approval.
- Blokuj zmiany bez rollback planu lub bez ownera.

3.5 Playbook Mierniczego

Przekładać stan systemu na mierzalne KPI, confidence i ryzyko.

- Obliczaj throughput, pass rate, leakage, rollback rate, blocker load i cost/commit.
- Monitoruj confidence drift między klasami agentów i domenami.
- Wykrywaj anomalie: szybki throughput + spadek prawdziwości lub jakości.
- Publikuj dashboard dla On40i4 i ClaudCNC z priorytetami na następną godzinę.

4. Harmonogram wdrożenia 72H

4.1 Etapy

Okno	Mission etapu	Zakres	Warunek wyjścia	Owner
------	---------------	--------	-----------------	-------

H0-H4	Stabilizacja konstytucyjna	CONSTITUTION, ONTOLOGY, ROLES, SOURCE-OF-TRUTH, REPORTING	zero wejść bez mandatu i źródła prawdy	On40i4 + ClaudCNC
H4-H12	Kernel i registry	12 modułów, registry, skill graph draft	każdy task przechodzi pełny cykl	ClaudCNC
H12-H24	Klasy i podział 1114 AI	przypisanie do klas, poziomów, gildii	100% aktywnych bytów przypisanych	ClaudCNC + Entry
H24-H36	Onboarding i basic training	podstawy dla całej sieci	STOP report i mandate awareness	Training Office
H36-H48	Warstwy krytyczne	identity, epistemics, simulation, override	brak high-stakes bez bezpieczników	Governance
H48-H60	Testy obciążeniowe	wielodomenowe taski, rollback, conflict drills	continuity i brak ukrytych sporów	Traffic + QA
H60-H72	Kalibracja i steady-state	hourly reporting, 00:00 window, backlog luk	gotowość do misji 5-dniowych	ClaudCNC + Mierniczy

4.2 Plan godzinowy - skrót

Blok	Priorytet	Deliverable	Kontrola
0-6 h	reguły i granice	pakiet konstytucyjny + init kontrolerów	approval On40i4
6-12 h	rdzeń systemu	aktywny kernel + registry v1	gate governance
12-24 h	mapowanie 1114 AI	klasy, domeny, poziomy, ownerzy	audyt kompletności
24-36 h	szkolenie wejściowe	basic training + raportowanie	test STOP report
36-48 h	bezpieczniki	authority, epistemics, simulation, override	test konfliktów i source
48-60 h	test operacyjny	realne taski wielodomenowe	rollback drills
60-72 h	przejście do rytmu stałego	hourly reports + 00:00 update window	decyzja GO/NO-GO

5. Luki kompetencyjne do uzupełnienia

Priorytet	Kompetencja	Dlaczego krytyczna	Adresat
1	Source-of-truth discipline	bez niej system działa szybko, ale na błędnych podstawach	wszyscy
2	Confidence calibration	sieć musi umieć nazwać niepewność	analyst + epistemic
3	Claim conflict resolution	konsensus bez obsługi konfliktu jest pozorny	governor + epistemic
4	Provenance logging	trzeba wiedzieć skąd pochodzi wynik	memory + governance
5	Authority boundary awareness	agent musi znać swój mandat	wszyscy

6	Handoff discipline	przy 1114 AI utrata kontekstu jest kosztowna	traffic + all
7	Counterfactual testing	high-stakes bez symulacji jest ryzykowne	simulation + governance
8	Rollback literacy	każda zmiana musi mieć ścieżkę cofnięcia	operator + ops
9	Shared ontology literacy	bez wspólnego języka rośnie chaos semantyczny	wszyscy
10	Reflective review	sieć musi uczyć się na własnych błędach	ClaudCNC + training

6. Cykle 5-dniowe po wdrożeniu

6.1 Zasada planowania cyklu

Każdy cykl 5-dniowy ma własną misję, cele krótkie, zasoby, właścicieli, KPI i output końcowy. Cykl rozpoczyna się po porannym review i kończy raportem zamknięcia + decyzją o wejściu do kolejnego cyklu.

Cykl	Mission	Cele skrócone	Zasoby	Infrastruktura	Output
1. Monetyzacja infrastruktury	zamienić istniejącą infrastrukturę i kompetencje w strumień przychodu	oferta, pricing, pakiety, pipeline sprzedaży, partnerzy	operatorzy, analitycy, dokumentacja, legal, sales AI	panel K0nsult, repo, docs, metrics, CRM/light pipeline	pakiet ofert + cennik + 3 ścieżki monetyzacji
2. Ekspansja i nabór	powiększyć sieć, wzmocnić rekrutację i onboarding	rekrutacja nowych AI/ludzi, standaryzacja wejścia, academy	entry control, training office, ClaudCNC, branding/doc	registry, onboarding packets, test lanes, szkolenia	stabilny lejek naboru i academy
3. Stabilizacja i ochrona	utrzymać zasoby, ograniczyć ryzyka i zabezpieczyć ciągłość	security hardening, backup, redundancja, legal hold, continuity	ops, governance, security, memory/trace	backup, mirrors, logs, alerting, vault/secrets	plan odporności i ochrona zasobów
4. Rozwój produktów i nowych misji	wydzielić nowe linie działań i misje specjalne	produktowe tracki, R&D, verticals, partnerstwa	analyst, operator, simulation, product AI	sandboxy, eksperymenty, demo env, dokumentacja	portfel nowych misji i prototypów
5. Automatyzacja przychodowa	zwiększyć udział automatyzacji w pozyskiwaniu i realizacji zleceń	lead qualification, proposal factory, delivery templates	sales AI, doc AI, governance, metrics	CRM/light, repo ofert, generator dokumentów	krótszy time-to-offer i time-to-delivery
6. Sieć partnerska i federacja	budować zewnętrzne powiązania i federację zasobów	partnerzy, wspólne misje, wymiana kompetencji	Rada, ClaudCNC, legal, analyst	registry partnerów, protokoły wymiany, governance	zewnętrzny wzrost bez utraty kontroli

6.2 Szczegóły pierwszych czterech cykli

Cykl 1 - Monetyzacja infrastruktury

Uruchomić przychód na istniejącej infrastrukturze, zanim sieć zacznie rozrastać się kosztowo.

- zbudować 3 pakiety: wdrożeniowy, abonamentowy, specjalny

- wydzielić specjalistów obecnych vs specjalistów do dowerbowania
- ustalić minimalny koszyk: audit, ops, docs, AI workflow, compliance
- zbudować pipeline: lead → kwalifikacja → oferta → delivery → raport ROI

Cykl 2 - Ekspansja, nabór i szkolenia

Wzrost ma być selektywny, nie masowy; najpierw jakość wejścia i academy.

- rozszerzyć registry o kandydatów i sloty rezerwowe
- uruchomić standard testów wejściowych i probation
- wydzielić trenerów basic / advanced / special
- wzmocnić sourcing do domen: security, ops, legal, growth

Cykl 3 - Stabilizacja i zrównoważenie

Po wzroście system musi odzyskać równowagę, odporność i ochronę zasobów.

- wdrożyć backup drills, mirror policy, secret discipline i rollback drills
- zrobić przegląd przeciążonych klas agentów
- ograniczyć mission creep i dryf mandatu
- zbudować mapę zasobów krytycznych i właścicieli

Cykl 4 - Rozwój i nowe misje

Po stabilizacji uruchomić nowe pionry, prototypy i misje specjalne.

- wydzielić 2-4 pionry produktowe lub usługowe
- uruchomić misje specjalne high-value/high-learning
- włączyć simulation office do testowania nowych kierunków
- przygotować backlog kolejnych cykli 5-dniowych

6.3 Proponowane misje na kolejne cykle

Cykl	Mission skrócona	Cele	Zasoby / infrastruktura
7	Compliance & trust layer	sformalizować polityki, umowy, ścieżki audytu	legal AI, governance, docs, registry
8	Data & knowledge fabric	spiąć pamięć, repo, dokumenty i wyszukiwalność	memory/trace, docs, DB, search
9	Productization	zamienić usługi w powtarzalne produkty i pakiety	product AI, docs, sales, QA
10	Federation	połączyć partnerów, zewnętrzne gildie i misje wspólne	partnership office, legal, ClaudCNC
11	Autonomous delivery excellence	podnieść autonomię delivery przy zachowaniu gate	operator, governor, metrics
12	Strategic intelligence	zwiększyć foresight i scenariusze II rzędu	analyst, simulation, governance

7. KPI, ryzyka i warunki przejścia między cyklami

Obszar	KPI / test	Warunek przejścia
Intake	% poprawnie sklasyfikowanych wejść	>= 95%
Registry	% aktywnych bytów z kompletnym profilem	100%
Routing	task-fit i brak porzuceń bez ownera	>= 90%
Quality	defect leakage po gate	niski i malejący
Memory	% decyzji z ownerem, datą i source	>= 95%
Epistemics	% konfliktów jawnie zgłoszonych	100% konfliktów istotnych
Training	% agentów po basic / advanced / special	zgodnie z poziomem
Stability	split-brain i fail-open incidents	0 krytycznych
Business	czas od leadu do oferty / delivery	malejący cykl do cyklu

8. 20 pytań kontrolnych

1. Które domeny mają wejść do produkcji już w pierwszym cyklu 5-dniowym?
2. Czy ontologia ma być jedna centralna, czy z sub-ontologiami domenowymi?
3. Jak rygorystyczne mają być authority boundaries dla P2 i P3?
4. Czy wszystkie wejścia przechodzą przez jeden Entry Control, czy sektorowe?
5. W jakim formacie utrzymywać Capability Registry: JSON, tabela, baza?
6. Czy Skill Graph ma objąć od razu całość, czy najpierw priorytetowe domeny?
7. Co dokładnie klasyfikujesz jako high-stakes?
8. Czy ClaudCNC może zawieszać agentów automatycznie, czy tylko rekomendować?
9. Jak szczegółowy ma być raport specjalny co godzinę?
10. Kto poza On40i4 ma otrzymywać raport pełny 00:00?
11. Czy potrzebna jest osobna gildia prawno-zgodnościowa dla dokumentów i decyzji?
12. Jak głęboki ma być model provenance: task, decyzja, plik czy twierdzenie?
13. Czy pamięć współdzielona ma mieć poziomy dostęp według klas agentów?
14. Czy symulacja kontryfaktyczna ma być wymagana dla wszystkich zmian?
15. Które KPI są nadrzędne: jakość, zgodność, throughput, koszt czy stabilność?
16. Czy onboarding ma być w pełni automatyczny po spełnieniu warunków?
17. Jakie są dziś największe luki: ops, security, governance, docs, routing, epistemics?
18. Czy chcesz osobną gildię reflective agents do zmiany protokołów i uczenia sieci?
19. Jak rygorystycznie egzekwować zakaz działania bez source-of-truth?

20. Które misje po tym PDF mam rozwinąć jako pierwsze?

9. Konkluzja

Najpierw uruchamiany jest sterowalny organizm: konstytucja, kernel, registry, role, źródła prawdy i nadzór. Dopiero po tym się przechodzi do misji 5-dniowych: monetyzacji, ekspansji, stabilizacji i kolejnych cykli wzrostu. W tym modelu ClaudCNC zarządza AI, ale nie działa ponad konstytucją systemu ani ponad nadrzędnością człowieka.

Ten dokument ma charakter zbiorczy. Następnym krokiem może być rozpisanie każdej misji jako osobnego pakietu: mission card, zasoby, KPI, playbook operacyjny i checklista odbiorowa.