

EAOS

Enterprise AI Operating System

سکوی هوشمند فرایند و تولید سامانه‌های سازمانی

AEPB – AI-Native Enterprise
Process & ERP Builder



- طراحی و اجرای فرایند بر پایه BPMN 2.0
- تولید خودکار ERP، فرم، API و پایگاه داده
- هوش مصنوعی مستقل از فروشنده
- امنیت، حاکمیت و چندمستأجری از روز اول

از متن، تا سامانه در حال اجرا

سکوی بومی - قابل استقرار درون سازمانی و در محیط ایزوله

AEPB یک محصول واحد است که به‌جای خرید چند ابزار جدا، **هشت سکوی وابسته** را زیر یک متامدل سازمانی و یک زنجیرهٔ تحویل پیوسته جمع می‌کند. خروجی هر بخش، ورودی بخش بعدی است.

۱

مدیریت فرایند کسب‌وکار

BPMS

طراحی، اعتبارسنجی، شبیه‌سازی و اجرای واقعی فرایند با استاندارد BPMN 2.0 — نه فقط ترسیم.

۲

موتور تصمیم و پرونده

DMN · Case

جدول‌های تصمیم استاندارد DMN و مدیریت پرونده به‌سبک CMMN با تسک‌های موردی و نقاط عطف.

۳

تولید سامانهٔ سازمانی

ERP Builder

از یک توضیح زبان طبیعی: مدل داده، فرم، API، CRUD، داشبورد و ماژول ERP ساخته و روی پایگاه‌دادهٔ زنده مستقر می‌شود.

۴

هستهٔ هوش مصنوعی

AI Core

درگاه یکپارچه LLM (ابری، محلی یا آفلاین)، معمار فرایند، تحلیلگر، اعتبارسنج و ترمیم‌گر خودکار.

۵

تحلیل، داشبورد و کاوش فرایند

BI · Mining

شاخص‌ها، زمان چرخه، گلوگاه‌ها و کاوشی فرایند بر پایهٔ رخدادهای واقعی اجرا — نه داده‌های نمایشی.

۶

یکپارچگی سازمانی و صنعتی

Integration · OT

کانکتورهای REST، SOAP، GraphQL، Kafka و MQTT و لایهٔ صنعتی OPC-UA، Modbus، IEC-104 و SCADA.

۷

حاکمیت امنیت و توسعهٔ امن

Security · DevSecOps

مدل‌سازی تهدید، ریسک، انطباق، پویش راز و وابستگی و تولید SBOM — درون‌ساخت، نه افزونه.

۸

کارخانهٔ محصول و پک‌های دامنه

Factories

۳۴ پک آمادهٔ سازمانی، دولتی و انرژی، کارخانهٔ محصولات امنیتی و کارخانهٔ اپلیکیشن.

مسئلهٔ اصلی، نبود ابزار نیست؛ مسئله این است که خروجی هیچ ابزاری ورودی ابزار دیگر نمی‌شود. مدل فرایند به پایگاه‌داده وصل نیست، فرم به فرایند وصل نیست، و داشبورد از دادهٔ واقعی اجرا تغذیه نمی‌شود. این سامانه دقیقاً روی همین اتصال‌ها بنا شده است.

شکاف اصلی سازمان‌ها میان «آنچه تحلیل و مستند می‌شود» و «آنچه واقعاً اجرا می‌شود» است. سند فرایند در یک ابزار می‌ماند، سامانه در ابزار دیگری ساخته می‌شود، و پس از مدتی این دو هیچ نسبتی با هم ندارند.

با این سامانه

فرایند اجرایی

همان مدل BPMN مستقیماً اجرا می‌شود

یک متامدل واحد سازمانی

UEMM – همه ماژول‌ها یک مدل را مصرف می‌کنند

تولید از متن در چند دقیقه

مدل داده، فرم، API و داشبورد خودکار

کاوش از رخداد واقعی

زمان چرخه و گلوگاه از اجرای زنده

امنیت از روز اول

چندمستأجری، RBAC، ممیزی و SBOM درون‌ساخت

وضعیت امروز

فرایند روی کاغذ و ویزیو

چند فایل جدا، بدون اجرا

هر سامانه یک جزیره

هر ماژول مدل داده خودش را دارد

ماه‌ها کدنویسی برای هر ماژول

از تحلیل تا تحویل، چرخه بلند

گزارش از روی حدس

شاخص‌ها دستی و با تأخیر

امنیت، وصله بعد از تحویل

افزوده‌شده در پایان پروژه

Vendor-Neutral

بدون قفل فروشنده هوش مصنوعی

Multi-Tenant

چندمستأجری از اولین جدول

BPMN-First

مدل استاندارد، منبع واحد حقیقت

AI-Native

هوش، هسته محصول است نه افزونه

جریان هسته محصول یک زنجیره پیوسته است: هر گام خروجی ماشین‌خوان تولید می‌کند که ورودی گام بعد است. هیچ گامی «صادرات دستی به ابزار بعدی» ندارد.

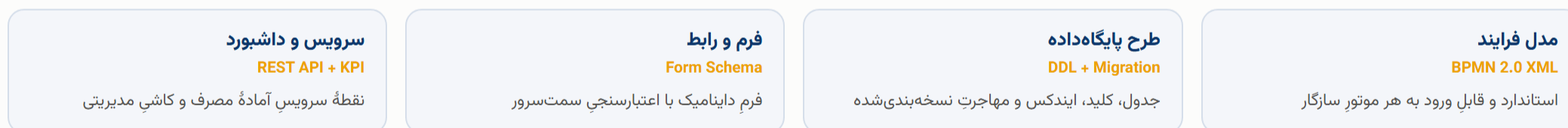
زنجیره تولید (North Star)



چرخه عمر فرایند



آنچه از یک جمله تولید می‌شود



چرخه عمر داده: کشف ← مدل سازی ← طبقه بندی ← ذخیره ← حاکمیت ← تحلیل ← بایگانی.
طبقه بندی داده و تشخیص داده شخصی (PII) در همین مسیر انجام می‌شود.

قاعده سخت گیرانه: هیچ مدل BPMN ای بدون عبور از اعتبارسنج ساختاری ذخیره نمی‌شود. خروجی هوش مصنوعی هم دقیقاً از همین دروازه رد می‌شود — استثنایی وجود ندارد.

معماری در ۹ لایه تعریف شده و امروز به صورت یک **Modular Monolith** با مرزهای بسته هر دامنه پیاده شده است — به گونه ای که هر دامنه بدون بازنویسی به یک ریزسرویس مستقل تجزیه شود.

L1	لایه تجربه	Studio تحت وب (Next.js / React / TS) · ویرایشگر گرافیکی BPMN · فرم داینامیک · پورتال موبایل
L2	لایه فرایند	طراح BPMN · موتور اجرا (چندتوکنی) · موتور تصمیم DMN · موتور پرونده Case · شبیه سازی
L3	لایه داده	کشف مدل داده · تولید Schema و مهاجرت · لایه انتزاع پایگاه داده · حاکمیت و کیفیت داده
L4	لایه یکپارچگی	دروازه API · هاب یکپارچگی (REST · SOAP · GraphQL · Kafka · MQTT · JDBC) · Webhook با امضا
L5	لایه هوش مصنوعی	درگاه LLM · مسیریاب مدل · معمار و تحلیلگر فرایند · RAG · گراف دانش · چارچوب عامل ها
L6	لایه تحلیل	سازنده داشبورد · موتور شاخص · کاوش فرایند · انبار داده و ETL
L7	لایه حاکمیت	سرویس امنیت · موتور سیاست (RBAC / ABAC) · ممیزی تغییرناپذیر · انطباق و مدل سازی تهدید
L8	لایه زمان اجرا	باس رخداد · زمان بند و تایمر · اعلان · سرویس فایل · حافظه نهان · جست و جو
L9	لایه زیرساخت	Kubernetes · Docker · PostgreSQL · Redis · Kafka · MinIO · Elasticsearch · Prometheus

چندزبانه در جای درست: هسته Python/FastAPI · موتور اجرای Go · تجربه کاربری Next.js — هر کدام در حوزه قوت خود.

هر اتصال بیرونی، پیش فرض آفلاین دارد: Kafka، MinIO، Elasticsearch، پایگاه برداری و OIDC در نبود سرویس، به حالت درون فرایندی قطعی برمی گردند.

ابتدا یکپارچه ماژولار، سپس ریزسرویس: مرز پکیج ها از روز اول تمیز است؛ تجزیه یک تصمیم عملیاتی است نه یک بازنویسی.

دوازده موتور، هرکدام با مرز، قرارداد و آزمون مستقل. هیچ موتوری مستقیماً در پایگاه داده موتور دیگر نمی نویسد؛ ارتباط از طریق قرارداد سرویس و **باس رخداد** انجام می شود.

موتور گردش کار

Workflow

اجرای چندتوکنی BPMN، انشعاب و همگرایی،
انتظار انسانی، نسخه بندی

عملیاتی

موتور تصمیم

DMN

جدول تصمیم با سیاست های UNIQUE، FIRST
و COLLECT و تجمیع؛ ارزیابی امن بدون اجرای
کد

عملیاتی

موتور پرونده

Case · CMMN

تسک موردی، نقطه عطف، درصد پیشرفت،
اجرای فرایند از داخل پرونده

عملیاتی

موتور فرم

Form

ساخت فرم از مدل داده + اعتبارسنجی
سمت سرور ارسال، نسخه بندی فرم

عملیاتی

موتور قاعده و سیاست

Policy

کنترل دسترسی نقش محور و صفت محور،
مجوزهای دانه ریز، سیاست چندمستأجری

عملیاتی

موتور زمان بند

Scheduler

رویدادهای تایمر (شروع، میانی و مرزی) با قالب
ISO 8601 و تیک قطعی

عملیاتی

موتور اعلان

Notification

اعلان درون سامانه ای، Webhook با امضای
HMAC، تلاش مجدد و نگه داشت

عملیاتی

موتور گزارش و تحلیل

Analytics

شاخص، زمان چرخه، توان عبور، کاوش فرایند،
خروجی CSV

عملیاتی

موتور هوش مصنوعی

AI

معمار، تحلیلگر، اعتبارسنج، ترمیم گر، بازیابی
مبتنی بر دانش و عامل ها

عملیاتی - هسته هوش قابل ارتقا

موتور شبیه سازی

Simulation

اجرای خشک، گزارش نقاط توقف، بازپخش
رخدادها

پایه

دوقلوی دیجیتال

Digital Twin

رجیستری دارایی صنعتی و نگاشت فرایند به
تجهیز

پایه - کانکتور شبیه سازی شده

موتور جست و جو و فایل

Search · File

جست و جوی چندموجودیتی و مدیریت فایل با
اتصال ذخیره ساز شیئی

عملیاتی

پوشش BPMN در این سامانه «ترسیمی» نیست؛ هر عنصر زیر واقعاً در زمان اجرا تفسیر و اجرا می‌شود و آزمون خودکار متناظر دارد.

گیت‌وی و مسیریابی

- **Exclusive** – انتخاب شاخه بر پایه شرط، با ارزیابی امن (بدون اجرای کد)
- **Parallel** – انشعاب و همگرایی واقعی (fork/join) با اجرای چندتوکنی
- مسیر پیش‌فرض و تشخیص **انشعاب ضمنی** به عنوان خطای مدل‌سازی

فعالیت‌ها و زیرفرایند

- **Call Activity** – زیرفرایند مستقل با تبادل متغیر ورودی/خروجی
- رویداد مرزی **قطع‌کننده** و **غیرقطع‌کننده** (یادآور بدون لغو تسک)
- انواع تسک: کاربر · سرویس · اسکریپت · قاعده کسب‌وکار · ارسال · دریافت · دستی
- اتصال تسک سرویس به **هاب یکپارچگی** و ثبت نتیجه در متغیرها

رویدادها

- **تایمر** – شروع، میانی و مرزی (ISO-8601) با تیک قطعی زمان‌بند
- **پیام** – همبسته‌سازی یک‌به‌یک با کلید کسب‌وکار و انتقال متغیر
- **سیگنال** – انتشار یک‌به‌چند به همه نمونه‌های منتظر
- **خطا** – پرتاب در پایان و گرفتن روی مرز زیرفرایند (try/catch)
- **پرتاب میانی و رویداد شروع از پیام/سیگنال** (Choreography)
- **Terminate** – پایان قطعی همه شاخه‌های موازی

چرخه عمر و ابزار

- ورود و خروج XML استاندارد، سازگار با **Camunda / Flowable**
- ورود و خروج **DMN XML** برای جدول‌های تصمیم
- نسخه‌بندی، **تفاوت ساختاری** دو نسخه و **بازگردانی غیرمخرب**
- ترمیم خودکار گره‌های یتیم (تسک، رویداد، گیت‌وی، زیرفرایند)
- بازپخش، اجرای خشک و گزارش نقاط توقف پیش از استقرار

ویرایشگر گرافیکی کامل

مدل‌ساز استاندارد صنعتی با پالت کامل، ذخیره نسخه با حفظ چیدمان، و حالت **ویرایش** ↔ **اجرا** با هایلایت زنده توکن روی دیاگرام.

چیدمان تمیز سمت‌سرور

فرایندهای تولیدشده توسط هوش مصنوعی با **چیدمان لایه‌ای** **چپ‌به‌راست** و مختصات کامل گرافیکی تولید می‌شوند – نه چیدمان خودکار خام در مرورگر.

اجرای موازی و بازگشتی

موتور، چند توکن را هم‌زمان پیش می‌برد؛ زنجیره پرتاب/دریافت و بازگشت زیرفرایند با درین کنترل‌شده و محافظ در برابر حلقه بی‌پایان اداره می‌شود.

هوش مصنوعی در این سامانه یک لایه افزوده نیست؛ اما **تصمیم‌گیرنده نهایی هم نیست**. هر خروجی هوشمند از یک دروازه قطعی عبور می‌کند و در صورت مردود شدن، ذخیره نمی‌شود.

قابلیت‌های هوشمند

معمار فرایند — متن ← BPMN با شاخه شرطی، اجرای موازی و رویدادهای زمان و پیام

تحلیلگر فرایند — یافته‌های عمل‌گرا: گیت‌وی بدون شرط، انشعاب ضمنی، وابستگی بیرونی، فرایند خطی

اعتبارسنج — بررسی ساختاری و معنایی پیش از هر ذخیره‌سازی

ترمیم‌گر — سیم‌کشی خودکار گره‌های یتیم و اصلاح ساختار

مستندساز و مترجم — تولید مستند فرایند، توضیح زبان طبیعی و ترجمه چندزبانه

چارچوب عامل‌ها — عامل‌های تخصصی + هماهنگ‌کننده چندعاملی با حافظه کوتاه/بلندمدت

پشته مستقل از فروشنده

درگاه مدل زبانی

LLM Gateway

یک نقطه ورود واحد؛ هیچ کد دامنه‌ای به کتابخانه یک فروشنده وابسته نیست

مدیر قالب دستور

Prompt Manager

قالب‌های نسخه‌دار و قابل ممیزی برای هر وظیفه

مسیریاب مدل

Model Router

انتخاب مدل بر پایه نوع وظیفه، هزینه و دسترس‌پذیری

تأمین‌کنندگان قابل تعویض

بدون مدل

قطعی و آفلاین

بدون هیچ وابستگی بیرونی — پیش‌فرض محیط ایزوله

Ollama / vLLM

مدل محلی

اجرای مدل روی زیرساخت خود سازمان

Anthropic / OpenAI

ابری

در صورت مجاز بودن سیاست سازمان

دانش و بازیابی

- **RAG** با تولید پاسخ مبتنی بر سند و ارجاع صریح به منبع
- **پایگاه برداری** با اتصال استاندارد و بازگشت خودکار به حالت درون‌فرایندی
- **گراف دانش** برای استخراج موجودیت و رابطه از متن

تعویض تأمین‌کننده، بدون تغییر کد

انتخاب ارائه‌دهنده فقط یک مقدار پیکربندی است. سازمان می‌تواند امروز کاملاً آفلاین کار کند و فردا یک مدل محلی را جایگزین کند، بدون آنکه هیچ فرایند یا ماژولی بازنویسی شود.

جایگاه هوش مصنوعی: دستیار است، نه تصمیم‌گیرنده. خروجی مدل همیشه از اعتبارسنج ساختاری رد می‌شود، نتیجه آن جدا از نتیجه قطعی نمایش داده می‌شود، و **تصمیم نهایی همواره بر عهده انسان است**.

کاتالوگ محصول ۲۰۰ ماژول با شناسه پایدار است. هر شناسه به یک محل مشخص در کد نگاشت شده و یک ماتریس ردیابی خودکار تضمین می‌کند هیچ ماژولی بدون کد نماند.

۱۰ کانکتور پایگاه داده MODULE ۰۶۷-۰۷۶ هشت درایور دیگر اعلام شده MySQL و PostgreSQL پیاده؛	۱۰ مدل سازی داده MODULE ۰۵۷-۰۶۶ کشف موجودیت و رابطه، تولید Schema و مهاجرت، طبقه بندی، حاکمیت، کیفیت	۱۰ تولید سامانه MODULE ۰۴۷-۰۵۶ ERP، اپلیکیشن، API، CRUD، سرویس، رابط، داشبورد، گزارش، بسته، استقرار	۱۰ فرایند هوشمند MODULE ۰۳۷-۰۴۶ معمار، تحلیلگر، اعتبارسنج، بهینه ساز، ترمیم، مستند ساز، مترجم	۱۶ فرایند و گردش کار MODULE ۰۲۱-۰۳۶ طراح، تجزیه گر، اعتبارسنج، موتور اجرا، نسخه، شبیه سازی، بازپخش، استقرار	۲۰ سکوی هسته MODULE ۰۰۱-۰۲۰ هویت، مستأجر، سیاست، ممیزی، اعلان، فایل، زمان بند، دروازه، باس رخداد
۱۰ توسعه امن MODULE ۱۲۷-۱۳۶ مخزن، ساخت، استقرار، SAST، SBOM، وابستگی، راز، DAST	۱۰ هوش مصنوعی و مدل زبانی MODULE ۱۱۷-۱۲۶ درگاه، مدیر قالب، مسیریاب، RAG، پایگاه برداری، عامل ها، گراف دانش	۱۰ صنعتی و عملیاتی MODULE ۱۰۷-۱۱۶ IEC-104، Modbus، OPC-UA، PLC، SCADA، DNP3، Historian، دوقلوئی دیجیتال	۱۰ یکپارچگی سازمانی MODULE ۰۹۷-۱۰۶ REST واقعی، SOAP، GraphQL، Kafka، MQTT، فایل، ایمیل و Webhook	۱۰ تحلیل و هوش کسب و کار MODULE ۰۸۷-۰۹۶ داشبورد، شاخص، کاوش فرایند، پیش بینی، گزارش، انبار داده و ETL	۱۰ فرم و محتوا MODULE ۰۷۷-۰۸۶ فرم ساز، فرم هوشمند، موتور داینامیک، اعتبارسنجی، نسخه، قالب
۱۰ کارخانه اپلیکیشن MODULE ۱۹۱-۲۰۰ جریان داده، نگاشت OSI، نقشه سامانه، معماری، ریزسرویس، پایگاه داده، رابط، API، زیرساخت	۱۰ کارخانه محصول سایبری MODULE ۱۸۱-۱۹۰ SOAR، SIEM، DLP، PAM، XDR، EDR، اسکرن، هوش تهدید، کشف دارایی	۱۰ پک های انرژی MODULE ۱۷۱-۱۸۰ نیروگاه، تولید، انتقال، توزیع، GIS، قطعی، تعمیرات، پیمانکار، مرکز عملیات	۸ پک های دولتی MODULE ۱۶۳-۱۷۰ مکاتبات، اتوماسیون سند، خدمات شهروندی، شکایات، مجوز، کمیته، مقررات	۱۶ پک های سازمانی MODULE ۱۴۷-۱۶۲ منابع انسانی، حقوق، مالی، بودجه، تدارکات، قرارداد، انبار، دارایی، CRM	۱۰ امنیت سایبری MODULE ۱۳۷-۱۴۶ انطباق، مدل تهدید، ریسک، آسیب پذیری، داشبورد، Zero Trust، دارایی

قابلی — ساختار تولید می‌شود، منطق عمیق دامنه در نقشه راه

قطعی و شبیه سازی شده — آفلاین کار می‌کند، سرویس واقعی پشت همان رابط

عملیاتی — منطق واقعی و آزمون شده

پک‌های دامنه و کارخانه‌ها روی همان زنجیره تولید صفحه پیش سوارند: هر پک یک **نقشه سامانه** تولید می‌کند که بلافاصله قابل استقرار و اجراست.

خط تولید محصول امنیتی از مدل جریان داده



پک ۱۶

پک‌های ERP

منابع انسانی · حقوق و دستمزد · مالی · حسابداری · بودجه · تدارکات · مدیریت قرارداد · انبار · انبارداری · مدیریت دارایی · ناوگان · مدیریت پروژه · دفتر مدیریت پروژه · CRM · مدیریت تأمین‌کننده · خدمات مشتری

پک ۸

پک‌های دولتی

مکاتبات اداری · اتوماسیون اسناد · خدمات شهروندی · مدیریت شکایات · صدور مجوز · حاکمیت گردش کار · مدیریت کمیته‌ها · مدیریت مقررات

پک ۱۰

پک‌های انرژی و وزارت

مدیریت نیروگاه · دارایی تولید · انتقال GIS · مدیریت قطعی · مدیریت تعمیرات · مدیریت پیمانکاران · مرکز توزیع · یکپارچگی عملیات اضطراری · مدیریت پروژه انرژی

محصول ۱۰

کارخانه محصول سایبری

XDR · EDR · SOAR · SIEM · DLP · PAM · اسکنر آسیب‌پذیری · هوش تهدید · کشف دارایی · مدیریت دارایی سایبری

پک ۱۰ مولد

کارخانه اپلیکیشن

طراح جریان داده · نگاشت OSI · نقشه سامانه · مولد معماری · مولد ریزسرویس · مولد پایگاه‌داده · مولد رابط کاربری · مولد API · مولد زیرساخت · هماهنگ‌کننده استقرار

مثال: ورودی «یک سکوی مدیریت دسترسی ممتاز بساز» ← خروجی: سرویس مخزن رمز، پایش نشست، گردش کار تأیید، موتور سیاست دسترسی، چرخش اعتبارنامه، داشبورد گزارش و سرویس ممیزی — به همراه مدل تهدید STRIDE و نگاشت کنترل.

صادقانه: پک‌های دامنه امروز یک **نقشه ساختاری کامل و قابل استقرار** تولید می‌کنند، اما منطق عمیق هر دامنه (مثلاً قواعد کامل حقوق و دستمزد) در نقشه راه است — نه در محصول امروز.

پنج سناریوی واقعی که امروز روی همین سکو قابل پیاده سازی‌اند. ستون «آنچه سامانه می‌سازد» دقیقاً همان چیزی است که به صورت خودکار تولید و مستقر می‌شود.

سناریو	ورودی	آنچه سامانه می‌سازد	خروجی عملیاتی
مدیریت پیمانکاران و قراردادهای	ثبت درخواست، ارزیابی صلاحیت، تأیید چندمرحله‌ای، عقد قرارداد، صورت وضعیت و تسویه	فرایند چندمرحله‌ای با گیت‌وی تأیید، تایمر SLA روی هر مرحله، فرم‌های داینامیک و پرونده پیمانکار	کارتابل زنده تأییدکنندگان، هشدار تأخیر، و گزارش زمان چرخه واقعی هر مرحله
مکاتبات اداری و اتوماسیون اسناد	ثبت نامه، ارجاع، پاراف، امضا، بایگانی و پیگیری	فرایند ارجاع با مسیر سازمانی، پرونده مکاتبه، جست و جوی چندموجودیتی و ممیزی تغییرناپذیر	پیگیری دقیق سرنوشت هر نامه و گزارش تأخیر واحدها
مدیریت قطعی و تعمیرات شبکه	اعلام خرابی، اعزام گروه، تعمیر، بازگردانی سرویس و ثبت دارایی	پیوند فرایند به رجیستری دارایی صنعتی و دوقلوی دیجیتال، رویداد پیام از سامانه SCADA، تایمر مرزی تعهد	زمان بازگردانی سرویس، گلوگاه اعزام، و نقشه دارایی درگیر
تولید محصول امنیتی از مدل جریان داده	توصیف نیاز امنیتی سازمان به زبان طبیعی	مرزهای اعتماد، مدل تهدید STRIDE، نگاشت کنترل به NIST/ISO/CIS، و نقشه ریزسرویس‌ها	بسته معماری و استقرار محصول (مثلاً SIEM یا PAM) به همراه گزارش انطباق
ماژول‌های ERP مالی، انبار و منابع انسانی	توضیح دامنه و موجودیت‌های اصلی	کشف موجودیت و رابطه، تولید Schema و مهاجرت، فرم و CRUD و API، و داشبورد مدیریتی	ماژول در حال اجرا روی پایگاه داده واقعی — با اعتبارسنجی سمت سرور و ماسک داده شخصی

نکته کلیدی: در هر پنج سناریو، داشبورد از رخدادهای واقعی اجرا تغذیه می‌شود — نه از ورودی دستی یا داده نمایشی.

چندمستأجری: هر سازمان، معاونت یا شرکت تابعه می‌تواند فضای داده کاملاً جدا داشته باشد؛ جداسازی در سطح هر رکورد اعمال می‌شود.

چندزبانه: پیام‌ها و خطاها با شناسه پایدار در فارسی، انگلیسی و عربی — با امکان افزودن زبان جدید بدون تغییر کد.

یک سکوی سازمانی وقتی موفق است که هر ذی‌نفع چیز مشخصی از آن به‌دست آورد – نه اینکه همه یک داشبوردهای مشترک ببینند.

ذی‌نفع	آنچه به‌دست می‌آورد	ذی‌نفع	آنچه به‌دست می‌آورد
مدیر ارشد و هیئت‌مدیره	تصویر مدیریتی از عملکرد فرایندها و زمان واقعی چرخه، بر پایهٔ رخداد اجرا	توسعه‌دهنده	API نسخه‌دار و خودتوصیف، مستند خودکار OpenAPI، و نقطهٔ اتصال برای هر سرویس بیرونی
مدیر فناوری اطلاعات	یک سکوی واحد به‌جای چند ابزار جدا؛ استقرار درون‌سازمانی و بدون قفل فروشنده	افسر امنیت	چندمستأجری، کنترل دسترسی نقش و صفت‌محور، ممیزی تغییرناپذیر، ماسک دادهٔ شخصی و SBOM
تحلیلگر کسب‌وکار	از توصیف فارسی به مدل اجرایشدن در چند دقیقه، با یافته‌های خودکار کیفیت مدل	ممیز داخلی و ناظر	دفتر ممیزی کامل با شناسهٔ همبستگی درخواست و خروجی قابل استخراج
طراح فرایند	ویرایشگر استاندارد BPMN، نسخه‌بندی، تفاوت ساختاری و بازگردانی غیرمخرب	مدیر عملیات	کارتابل اولویت‌دار، هشدار تأخیر، ارجاع و تشدید خودکار
معمار سامانه	کشف خودکار مدل داده، تولید ساختار و مهاجرت، و بستهٔ آمادهٔ استقرار	کاربر نهایی	فرم داینامیک با اعتبارسنجی سمت‌سرور و کارتابل ساده و فارسی

هر نقش، نمای خودش: آنچه هر کاربر می‌بیند با مجوزهای دانه‌ریز همان نقش تعیین می‌شود – از کارتابل سادهٔ کاربر نهایی تا دفتر کامل ممیزی. یک سامانه، چند تجربهٔ کاربری.

کارتابل مشترک: همهٔ تسک‌های انسانی همهٔ فرایندها در یک صندوق ورودی اولویت‌دار جمع می‌شوند – با مهلت، هشدار تأخیر، ارجاع و تشدید خودکار.

۱۵۰+

نقطهٔ API نسخه‌دار

۱۵

صفحهٔ کاری Studio

۳

زبان رابط (fa · ar · en)

۱۰

نقش کاربری تعریف‌شده

امنیت در این سکو یک مازولِ جداگانه نیست؛ در مسیرِ هر درخواست و هر رکورد اعمال می‌شود. آنچه در زیر آمده، پیاده‌شده و آزمون‌شده است.

هویت و دسترسی

- چندمستأجری از اولین جدول – هر رکورد شناسهٔ مستأجر دارد
- توکنِ مات داخلی، در کنارِ اتصالِ **OIDC** با تأییدِ امضای نامتقارن و کلیدِ عمومیِ برخط
- کنترل دسترسی نقش‌محور و صفت‌محور (RBAC/ABAC) با مجوزِ دانه‌ریز
- حالتِ احراز هویتِ اجباری، چرخشِ توکن، فعال/غیرفعال‌سازیِ کاربر

محافظت در زمان اجرا

- هدرهای امنیتی، سقفِ اندازهٔ بدنه و محدودسازیِ نرخ به‌ازای مستأجر
- اعتبارسنجی ورودی و شناسه‌های allowlist در CRUD داینامیک (ضدِ تزریق SQL)
- ماسکِ خودکارِ دادهٔ شخصی (PII) در مسیرهای خواندن
- رازها فقط از محیط یا مخزنِ راز – بدون افشا در لاگ

ممیزی و مشاهده‌پذیری

- دفترِ ممیزیِ تغییرناپذیر برای رخدادهای کلیدی + خروجیِ CSV
- شناسهٔ همبستگیِ درخواست در لاگ، پاسخ و بدنهٔ خطا
- Webhook با امضای HMAC، تلاش مجدد و سیاستِ نگاه‌داشت
- متریکِ Prometheus + ردیابیِ توزیع‌شدهٔ OpenTelemetry

توسعهٔ امن (DevSecOps)

- پویشِ ایستا و پویا، پویشِ وابستگی و پویشِ رازِ واقعی
- تولیدِ **SBOM** با قالبِ استاندارد CycloneDX
- مدل‌سازیِ تهدیدِ STRIDE، ارزیابیِ ریسک و نگاشتِ کنترل
- دروازهٔ پذیرشِ اجباری روی هر تغییر – بدون عبور سبز، ادغام ممکن نیست

استانداردهای هدف

ISO/IEC 27001	NIST 800-53	NIST CSF	OWASP API Security	OWASP Top 10	+OWASP ASVS L2
AES-256	TLS 1.3	Zero Trust	IEC 62443	CIS Controls	ISO/IEC 27002

کل استک با یک دستور بالا می‌آید. هر سرویس بیرونی یک **اتصال اختیاری** است: اگر در دسترس باشد استفاده می‌شود، و اگر نباشد سامانه به حالت درون‌فرایندی قطعی برمی‌گردد - به همین دلیل اجرای کاملاً آفلاین ممکن است.

اجزای زیرساخت

PostgreSQL

پایگاه داده اصلی - کل مجموعه آزمون روی آن سبز است

Redis

حافظه نهان و باس رخداد توزیع شده - روی سرویس واقعی اثبات شد

Kafka

باس رخداد سازمانی - اتصال آماده در کنار Redis

MinIO / S3

ذخیره ساز شیئی برای سرویس فایل

Elasticsearch

جست و جوی سازمانی با بازگشت خودکار به پایگاه داده

Keycloak

فدراسیون هویت با تأیید توکن امضا شده و نگاشت نقش به مجوز

Kong

دروازه لبه با مسیریابی، محدودسازی نرخ و سیاست دسترسی

Prometheus + Grafana

متریک و پایش؛ داشبوردهای آماده در نقشه راه

OpenTelemetry

ردیابی توزیع شده سرتاسری، خودغیرفعال شونده

Kubernetes

مانیفست های آماده استقرار به همراه دروازه لبه

حالت های استقرار

درون سازمانی

On-Prem

کاملاً روی زیرساخت خود سازمان

ابر خصوصی

Private

در مرکز داده اختصاصی

ترکیبی

Hybrid

هسته داخل، بار محاسباتی بیرون

ایزوله

Air-Gap

بدون هیچ اتصال اینترنتی

الزامات غیرکارکردی

- هدف دسترس پذیری ۹۹/۹۵٪ - مقیاس پذیری افقی - سرویس بدون حالت
- کانتینری شده و آماده Kubernetes با مانیفست نسخه دار
- مهاجرت نسخه بندی شده پایگاه داده - بدون تغییر دستی ساختار
- مشاهده پذیری اجباری: سلامت، متریک، لاگ ساختاریافته و ردیابی
- پیکربندی کامل از متغیر محیطی - بدون مقدار سخت کد شده

راه اندازی نمایشی: با پیکربندی پیش فرض و بدون هیچ سرویس بیرونی، سامانه بالا می‌آید و کل چرخه «متن -> فرایند -> استقرار -> اجرا» قابل نمایش است.

درصدها از **ممیزی درون‌سازمانی مازول‌ها** و خواندن واقعی کد آمده‌اند، نه از خوداظهاری. سامانه‌ای که مأموریتش حاکمیت فرایند بر پایه شاهد است، نمی‌تواند وضعیت خودش را بدون شاهد اعلام کند.

۲۰۰

ماژول ردیابی‌پذیر به کد

۳۶۱

آزمون خودکار سبز

۳۱

مهاجرت نسخه‌بندی‌شده

۱۶۳

فایل سورس هسته

۱۵

صفحه کاری Studio

+۱۵۰

نقطه API نسخه‌دار

عمق پیاده‌سازی (ممیزی مازول‌ها)

عمیق و تولیدی – منطقی واقعی، مدیریت حالت‌های لبه و آزمون متناظر

۱۰۹

قطعی و آفلاین – کار می‌کند و پایدار است، اما کم‌عمق؛ سرویس واقعی پشت همان رابط

۳۳

اعلام‌شده – رابط تعریف‌شده، نیازمند سامانه یا دراپور بیرونی

۱۲

مجموع نشان‌دارها ۱۵۴ مازول است؛ بقیه کاتالوگ به‌صورت تجمیعی (پک و کارخانه) پوشش داده شده.

آنچه روی سرویس واقعی اثبات شده

✓ **PostgreSQL** – کل مجموعه آزمون روی پایگاه‌داده تولیدی سبز شد – نه فقط مهاجرت‌ها

✓ **Redis** – انتشار رخداد روی سرویس واقعی و دریافت توسط مشترک مستقل

✓ **موتور Go** – پیشروی توکن، گیت‌وی شرطی و موازی – آینه موتور اصلی

✓ **Studio** – ساخت تولیدی کامل رابط کاربری و رندر زنده همه صفحات

✓ **مدل محلی** – مسیر کد اتصال به مدل محلی به‌صورت سرتاسری در دروازه سنجیده می‌شود

ردیابی‌پذیری: هر شناسه مازول در کد حضور دارد و یک بررسی خودکار تضمین می‌کند هیچ مازولی از ماتریس ردیابی جا نیفتد – نتیجه امروز: صفر مورد گم‌شده.

دروازه پذیرش: سبک‌سنجی، مهاجرت پایگاه‌داده، کل آزمون‌ها و اسموک اجرای واقعی – همگی سبز، و روی هر تغییر به‌صورت خودکار اجباری‌اند. ادعای «انجام شد» بدون عبور سبز پذیرفته نمی‌شود.

این صفحه عمده در کاتالوگ آمده است. آنچه ادعا نمی‌کنیم، به اندازه آنچه ادعا می‌کنیم اهمیت دارد؛ هر مورد زیر در نقشه راه صفحه بعد جای مشخصی دارد.

هوش پیش‌فرض، کلیدواژه محور است

تبدیل «متن به فرایند» و «متن به مدل داده» در حالت پیش‌فرض با نگاشت کلیدواژه کار می‌کند، نه درک زبانی عمیق. اتصال به مدل واقعی آماده است، اما پیش‌فرض محصول نیست.

کانکترهای صنعتی شبیه‌سازی شده‌اند

کانکترهای صنعتی شبیه‌سازی شده‌اند. امروز SCADA و OPC-UA، Modbus، IEC-104، DNP3 کلاپنت واقعی پروتکل هنوز پیاده نشده است.

پک‌های دامنه قالبی‌اند

۳۴ پک، ساختار کامل و قابل استقرار تولید می‌کنند اما منطق کامل دامنه (مثلاً قواعد حقوق و دستمزد یا استانداردهای حسابداری) را ندارند.

موتور مرجع اجرا هنوز Python است

موتور Go واقعی است و توکن را پیش می‌برد، اما اجرای عملیاتی همچنان بر عهده هسته Python است؛ واگذاری کامل یک تصمیم معماری و کار بزرگ است.

چند سرویس فقط رابط دارند

تشخیص نوری متن (OCR)، امضای دیجیتال و مدیریت ریزتنظیم مدل امروز فقط رابط تعریف شده‌اند و به موتور بیرونی نیاز دارند.

اپلیکیشن موبایل شروع نشده

پورتال موبایل در معماری تعریف شده اما هنوز پیاده‌سازی نشده است.

آزمون مقیاس انجام نشده

آزمون بار، نفوذ و کارایی در مقیاس عملیاتی هنوز اجرا نشده؛ اعداد دسترس‌پذیری، هدف طراحی‌اند نه نتیجه اندازه‌گیری.

داشبوردهای پیش تکمیل نشده

متریک و ردیابی برقرارند، اما مجموعه داشبوردهای آماده پیش هنوز تحویل نشده است.

چرا این صفحه را می‌نویسیم: فاصله میان ادعا و واقعیت، همان چیزی است که این محصول برای حذف آن در فرایندهای سازمانی ساخته شده. اگر درباره خودمان این فاصله را پنهان کنیم، هیچ دلیلی وجود ندارد که به گزارش ما درباره فرایندهای شما اعتماد شود.

شش موج ساخت تاکنون تکمیل شده اند و هرکدام پیش از آغاز موج بعد از دروازه پذیرش عبور کرده اند. موج هفتم، **عمق** است نه گستره: تبدیل آنچه امروز قالبی یا شبیه سازی شده است به منطقی واقعی.

موج های تکمیل شده



موج بعدی – شش اهرم عمق، به ترتیب ارزش



EAOS

Enterprise AI Operating System

از یک جمله فارسی، تا سامانه‌ای که واقعاً اجرا می‌شود

AEPB برای سازمان‌هایی ساخته شده که می‌خواهند فرایندهایشان را نه فقط ترسیم، بلکه اجرا، اندازه‌گیری و حاکمیت کنند – روی زیرساختِ خودشان، بدون قفلِ فروشنده، و با مرزی صادقانه میان آنچه امروز هست و آنچه در راه است.

استقرار درون‌سازمانی و ایزوله

هوش مصنوعی مستقل از فروشنده

تولید خودکار ERP

BPMN 2.0 · DMN · Case