شبكة الترحيل السيادي للذكاء عبر الويب

معمارية **KB-as-OS** لتوجيه الوكلاء إلى نماذج الذكاء الاصطناعي عبر الواجهات الرسومية، واستخراج المخرجات، والتحقق منها، وإعادة حقنها بجودة تشغيلية مقاربة لمسار **API**

زهير مساعف - Zouhair Moussaif

مشروع MOUSSAIF9B / Beyond AI Era - الإصدار البحثي الأول - يوليو 2026

الملخص

تقترح هذه الورقة معمارية **شبكة الترحيل السيادي للذكاء عبر الويب** (Sovereign WebConsole Relay Mesh - SWRM) بوصفها طبقة تشغيل معرفية تحول المتصفح من وسيط عرض إلى ناقل قدرات محكوم داخل منظومات الوكلاء. تنطلق المشكلة من أن عددًا متزايدًا من النماذج والخدمات الذكية يتيح أفضل أو أحدث قدراته عبر واجهة ويب تفاعلية، بينما تحتاج الأنظمة الوكيلة إلى عقود منظمة، وعزل للجلسات، وتوجيه قابل للتفسير، واستخراج موثوق، وسجل منشأ، وآلية لإعادة إدخال النتيجة في حالة الهدف. لا يكفي تقليد نقرات المستخدم؛ المطلوب هو بناء حاوية تشغيلية تجعل مسار الواجهة قابلاً للمراجعة والقياس والاسترجاع دون الادعاء بأن الواجهة الرسومية تساوي واجهة برمجية رسمية.

تقدم الورقة أربع إضافات: (1) **نظرية مساعف للترحيل السيادي** التي تفصل بين الوصول إلى القدرة واعتماد المعرفة؛ (2) **قانون استقلال الجوهر عن الواجهة** الذي يعزل المنطق المعرفي عن محولات المواقع؛ (3) **مقياس التكافؤ التشغيلي المقيد** لقياس مدى اقتراب المسار الرسومي من انضباط API؛ و(4) **بروتوكول إعادة الحقن الموثق** الذي يعيد النتيجة إلى الذاكرة العاملة كملاحظة خارجية موسومة لا كحقيقة نهائية. وتضم المعمارية أربعين HyperSkills موزعة على الإدراك المتصفحي، والتوجيه، والاستخراج، والتحقق، والأمن، والتعافي.

تقترح الورقة برنامج تقييم تجريبي يقيس أمان الجلسة، ودقة نقل الـPrompt، واكتمال الالتقاط، وحفظ الاستشهادات، ومقاومة انجراف الواجهة، وجودة إعادة الحقن، وكلفة المراجعة البشرية. وتخلص إلى أن قيمة النظام ليست في محاكاة الإنسان أو تجاوز ضوابط الخدمات، بل في إنشاء طبقة وسيطة سيادية تتيح استعمالًا مشروعًا ومقيدًا وقابلًا للتدقيق للقدرات المتاحة عبر الويب.

الكلمات المفتاحية: Agentic AI؛ Browser Automation؛ KB-as-OS؛ Web AI Consoles؛ HyperSkills؛ Provenance؛ Context Reinjection؛ UI Automation؛ Playwright؛ Microsoft UI Automation.

المساهمة المركزية: تحويل ناتج نموذج ويب من نص ظاهر في صفحة إلى كائن معرفي موثق يمر عبر التوجيه، والتحقق، والضغط، وإعادة الحقن، ضمن حدود تفويض وسياسة قابلة للتدقيق.

1. الإشكال البحثي وحدود المقاربة

1.1 من أتمتة النقر إلى هندسة القدرة

تتعامل معظم أنظمة أتمتة المتصفح مع الصفحة بوصفها سلسلة عناصر ينبغي إيجادها ثم تفعيلها. هذا التصور صالح للاختبارات والإجراءات المتكررة، لكنه غير كافٍ عندما يصبح المتصفح جزءًا من حلقة تفكير وكيلة. ففي هذه الحالة لا يقتصر المطلوب على فتح خدمة ذكاء اصطناعي وإرسال سؤال؛ بل يلزم تحديد سبب اختيار الخدمة، وسلامة الحساب والجلسة، ودرجة حساسية البيانات، وحفظ الصيغة الدقيقة للطلب، وتحديد لحظة اكتمال الجواب، واستخراج البنية والاستشهادات، ثم اختبار النتيجة قبل أن تؤثر في خطة الوكيل.

تزداد المشكلة لأن واجهات الويب عقود ضعيفة التثبيت: يمكن أن تتغير أسماء الأزرار، أو بنية الرسائل، أو آلية البث، أو وضع النموذج، أو شروط الاستخدام. ومن ثم فإن أي نظام يربط «العقل» مباشرة بمحددات CSS يصبح هشًا معرفيًا وتشغيليًا. تقترح SWRM فصلًا حاسمًا بين: **جوهر المهمة، وسياسة التوجيه، ومحول الخدمة، وأثر النتيجة في الذاكرة.** هذا الفصل يجعل إصلاح الواجهة عملية محلية لا إعادة كتابة للعقل الوكيل.

1.2 سؤال البحث

> **كيف يمكن بناء طبقة KB-as-OS تستخدم واجهات نماذج الذكاء الاصطناعي على الويب كموارد Agentic، مع تحقيق انضباط تشغيلي قريب من الـAPI، ومنع تسرب الجلسات والبيانات، وضمان أن المخرجات لا تدخل التفكير إلا بوصفها أدلة خارجية قابلة للتحقق؟**

1.3 الفرضيات

1. **فرضية الفصل:** فصل السياسة والمعرفة عن محولات الواجهة يقلل كلفة انجراف UI ويحسن قابلية إعادة الاستخدام.
2. **فرضية الحاوية:** تغليف كل طلب ونتيجة بعقد ثابت يحسن دقة النقل والمراجعة مقارنة بالتفاعل الحر.
3. **فرضية التحقق:** إعادة الحقن بعد محكمة ادعاءات تقلل انتشار أخطاء النماذج الخارجية داخل خطة الوكيل.
4. **فرضية الندرة:** التوجيه إلى أقل عدد كافٍ من لوحات الويب يحقق توازنًا أفضل بين الجودة، والخصوصية، والزمن، وكلفة الإفصاح.

1.4 ما لا تدعيه الورقة

لا تدعي المقاربة أن المتصفح يضمن ثباتًا أو تعاقدًا أو زمن استجابة مماثلًا للـAPI، ولا تقترح إخفاء الأتمتة أو تجاوز CAPTCHA أو MFA أو الحصص أو الدفع أو شروط الخدمة. كما لا تعد مخرجات نموذج آخر معرفة صحيحة لمجرد جودة صياغتها. معيار النجاح هو **الانضباط، والتوثيق، والتقييد، وقابلية المراجعة**، لا وهم التطابق التقني.

> **مبدأ تأسيسي:** الوصول إلى نموذج قوي لا يساوي امتلاك معرفة قوية؛ المعرفة تبدأ بعد إثبات المنشأ، وفحص الادعاء، وتحديد حدود الاستعمال.

2. الأساس التقني وحالة الفن

2.1 طبقة التحكم الدلالي

توفر Playwright واجهة موحدة لتشغيل Chromium وFirefox وWebKit، إضافة إلى قنوات متصفحات موسومة مثل Google Chrome وMicrosoft Edge [1]. وتسمح BrowserContexts بإنشاء جلسات مستقلة شبيهة بالملفات المتخفية، تفصل ملفات الارتباط والتخزين المحلي وحالة الجلسة [2]. تستفيد المعمارية من هذه الخصائص، لكنها تعيد توظيفها من إطار اختبار إلى إطار تشغيل معرفي: كل Context يصبح حدًا للثقة، وكل صفحة كيانًا مرتبطًا بمهمة ومحول وخطة احتفاظ.

تُفضل المحددات الدلالية المبنية على الأدوار والتسميات على الإحداثيات؛ لأن «زر الإرسال» كمعنى أكثر ثباتًا من موضعه البصري. وتنسجم هذه الفكرة مع نمط Page Object Model الذي يجمع محددات الواجهة في طبقة قابلة للصيانة بدل نشرها في منطق النظام [3]. غير أن SWRM توسع هذا النمط إلى **Service Adapter Contract** يضم الأصل المسموح، وصنف البيانات، وإشارات الاكتمال، وحالة مراجعة الشروط، وسياسة الاحتفاظ.

2.2 طبقة سطح المكتب في Windows

لا تقع كل التفاعلات داخل DOM. حوارات الملفات، وأذونات النظام، ونوافذ المتصفح الأصلية قد تحتاج إلى Microsoft UI Automation، وهو إطار إتاحة يوفّر وصولًا برمجيًا إلى معظم عناصر واجهة سطح مكتب Windows ويُتيح لأدوات الاختبار التفاعل معها [4]. لذلك تعمل المعمارية بمستويين: تحكم دلالي داخل الصفحة، وجسر UIA للحوارات الأصلية. ويُحظر استعمال ضغطات مفاتيح عامة حين تتوافر هوية عنصر أو نمط تحكم محدد.

2.3 بروتوكولات المتصفح

يوفر Chrome DevTools Protocol أدوات لفحص متصفحات Blink وتشخيصها وقياسها [5]، بينما يعرّف WebDriver واجهة محايدة للتحكم عن بعد في وكلاء المستخدم [7]، ويضيف WebDriver BiDi قناة ثنائية الاتجاه للأحداث والأوامر [8]. لا تجعل هذه البروتوكولات النظام «عالميًا» تلقائيًا؛ بل توفر طبقات قدرات متفاوتة. لذا يستخدم النظام **بصمة قدرة** لكل متصفح تحدد ما إذا كان التحكم يتم عبر Playwright أو CDP أو WebDriver/UIA أو مسار مراجعة بشرية.

2.4 قيد أمني حديث

أدخل Chrome منذ الإصدار 136 تشددًا على مفاتيح remote debugging عند استعمال مجلد البيانات الافتراضي، وطلب ربطها بمجلد بيانات غير قياسي [6]. يثبت ذلك أن «الاتصال بجلسة المستخدم» ليس تفصيلًا؛ بل سطح أمني يتغير. لذلك تعتمد الورقة ملفًا مخصصًا لكل حد ثقة، ولا تنقل قواعد بيانات كلمات المرور أو ملفات الجلسة إلى سياق الوكيل.

جدول 1 - تدرج التحكم المقترح

المرتبة	الآلية	سبب التفضيل	شرط الانتقال للأسفل
1	Roles / Labels / ARIA	ثبات دلالي وقابلية تدقيق	غياب العنصر دلاليًا
2	DOM scoped selectors	دقة داخل أصل موثوق	بنية ديناميكية أو Shadow/UI native
3	CDP / WebDriver	تشخيص وأحداث منخفضة المستوى	عدم كفاية التحكم داخل الصفحة
4	Windows UIA	حوارات ونوافذ أصلية	عنصر غير مكشوف
5	Visual fallback	حل أخير	مراجعة فورية وتحقق بعد الفعل

3. الإطار النظري الجديد

3.1 نظرية مساعف للترحيل السيادي

النظرية: كل قدرة معرفية خارجية تُستهلك عبر واجهة تفاعلية يجب أن تمر بثلاث سيادات مستقلة: سيادة الوصول التي تثبت التفويض، وسيادة الدليل التي تحفظ النص والمنشأ، وسيادة الأثر التي تقيد كيفية دخول النتيجة في هدف الوكيل. إذا غابت إحداها تحول المسار إما إلى وصول غير مشروع، أو معرفة بلا مصدر، أو تأثير غير قابل للضبط.

تُكتب حالة الترحيل على الصورة:

$$R = A \times E \times I$$

حيث A سلامة التفويض، وE اكتمال الدليل والمنشأ، وI سلامة إعادة الحقن. الصيغة ضربيّة لأن فشل أي مكون يجعل النتيجة غير صالحة للاعتماد، حتى لو كانت بقية المكونات مرتفعة.

3.2 قانون استقلال الجوهر عن الواجهة

القانون: ينبغي ألا يعتمد تمثيل المهمة ولا معايير صحة النتيجة على محددات خدمة بعينها. يُعرَّف الجوهر بواسطة QueryEnvelope وWebConsoleResult، بينما يحوّل Adapter هذين العقدين إلى عمليات محلية. ينتج عن ذلك أن تغيير زر أو بنية رسالة لا يغير منطق التوجيه أو محكمة التحقق أو الذاكرة.

$$\text{Cognitive Core} \perp \text{UI Adapter}$$

الرمز هنا دلالي: الاستقلال ليس انقطاعًا، بل منع انتقال هشاشة الواجهة إلى الطبقات المعرفية.

3.3 مقياس التكافؤ التشغيلي المقيد

تقترح الورقة مقياسًا لاختبار مدى اقتراب المسار الرسومي من انضباط API:

$$Q_{op} = (F \times C \times P \times V \times S) / (1 + D + H)$$

حيث F دقة نقل الـPrompt، وC ثقة اكتمال الجواب، وP اكتمال المنشأ، وV التحقق، وS عزل الجلسة، بينما D انجراف الواجهة، وH كلفة التدخل البشري. يمنع هذا المقياس وصف المسار بأنه «مكافئ» إن كانت النتيجة صحيحة أحيانًا لكن غير قابلة للتكرار أو فاقدة للمنشأ.

3.4 قانون إعادة الدخول السياقي

القانون: لا تُعاد النتيجة الخارجية إلى السياق بحجمها الخام ولا بوصفها تعليمات، بل تتحول إلى حزمة ادعاءات موسومة تحتوي المصدر، والحدود، والاستشهادات، والتعارضات، والثقة، والفعل المقترح. وهذا يحول دون أن يصبح نموذج الويب «سلطة خفية» داخل الوكيل.

صيغة إعادة الحقن:

ExternalObservation = {source, prompt_hash, claims, evidence, conflicts, limitations, confidence, recommended_use}

3.5 مبدأ الندرة التوجيهية

لا تعني القدرة على فتح عدة لوحات أن ذلك أفضل. كل لوحة إضافية ترفع احتمال الإفصاح، والتعارض، والتأخر، ومخالفة السياسة. ومن ثم يكون الافتراضي لوحة واحدة، وتضاف الثانية فقط إذا كانت قيمة التحقق الهامشية أعلى من كلفة الإفصاح والتعقيد.

4. المعمارية المرجعية وخط البيانات

4.1 أربع طائرات مترابطة

تتكون SWRM من أربع طائرات: **طائرة الإدراك المتصفحي**، **وطائرة التوجيه المعرفي**، **وطائرة الدليل والذاكرة**، **وطائرة الحوكمة والأمن**. الفصل بينها يسمح بتغيير المتصفح أو الخدمة أو سياسة المؤسسة دون تفكيك النظام كله.

Goal State → **Query Envelope** → **Policy Gate** → **Sparse Router** → **Browser Broker** → **Service Adapter** → **Capture** → **Falsification** → **Reinjection**

4.2 ممثلو التشغيل

المكوّن	المسؤولية	المخرج الحاكم
Goal Interpreter	تحويل المقصد إلى مهمة قابلة للتشغيل	Goal + constraints
Envelope Builder	تثبيت الطلب والحساسية والمهلة	QueryEnvelope + hash
Policy Gate	الترخيص والبيانات والشروط	allow / review / deny
Sparse HyperRouter	اختيار أقل خدمة كافية	ranked adapters
Browser/Profile Broker	تعيين المحرك وحد الثقة	browser context
Completion Detector	تمييز الاكتمال من البث الجزئي	state + confidence
Extractor	حفظ النص والبنية والاستشهادات	WebConsoleResult
Falsification Court	اختبار الادعاءات والفجوات	verdict
Context Compactor	ضغط دون إسقاط القيود	ExternalObservation
World-Effect Verifier	قياس أثر أي فعل لاحق	verified state change

4.3 العقدان الثابتان

العقد الأول هو QueryEnvelope: معرف المهمة، الهدف، نص السؤال الدقيق، الصنف، حساسية البيانات، شرط الحداثة، الخدمات المفضلة والممنوعة، الحد الأقصى للوحات، نمط الموافقة، مخطط الخرج، المهلة وسياسة الاحتفاظ. يحسب النظام SHA-256 للنص الذي سيملأ في الواجهة، ويقارن ما قبل التعبئة وما بعدها عند الإمكان.

العقد الثاني هو WebConsoleResult: معرف النتيجة والمهمة، اسم الخدمة، الوسم الظاهر للنموذج إن وجد، الأصل، إصدار المحول، بصمة الطلب، النص الخام، النص المطبّع، الاستشهادات، الزمن، ثقة الاكتمال، درجات الجودة، القرار السياسي والتحذيرات. العقد لا يفترض صحة الإجابة؛ بل يجعلها قابلة للفحص.

4.4 فصل الدليل عن التلخيص

يحفظ النظام أولًا النص المرئي الخام قبل أي تحسين. بعد ذلك تُجرى عملية تطبيع تحفظ العناوين والقوائم والكود والجداول والروابط والنفي والشك. ويُمنع على المستخرج «تصحيح» جواب النموذج؛ لأن التصحيح مرحلة تركيب لاحقة ويجب أن يبقى الفرق بين كلام المصدر واستنتاج الوكيل مرئيًا.

القاعدة: Raw before normalized; normalized before judged; judged before reinjected.

5. التوجيه الندري واختيار النموذج عبر الويب

5.1 متى يُستعمل المسار الرسومي؟

لا ينبغي أن يصبح المتصفح طريقًا افتراضيًا لكل سؤال. يُقبل التوجيه إذا طلب المستخدم خدمة بعينها، أو احتاجت المهمة قدرة فريدة متاحة في الويب، أو غاب مسار محلي/منظم معتمد، أو كان الغرض مقارنة عائلات نماذج، أو كانت الواجهة تقدم وضعًا تفاعليًا لا يعوضه المسار المتاح. ويُرفض إذا كان الهدف تفادي كلفة API أو الحصة أو حد السرعة أو الضوابط.

5.2 دالة الاختيار

$$S(c)=0.24C_{fit}+0.18Q+0.14P+0.10A+0.10U+0.08F+0.06R+0.05L+0.05T-\text{Risk-Drift}$$

تمثل الحدود: ملاءمة القدرة، الجودة المتوقعة، ملاءمة السياسة، جاهزية الجلسة، صحة الواجهة، ملاءمة الحداثة، جودة المنشأ، ملاءمة الكمون، وشفافية الكلفة. لكن هذه الدالة تأتي بعد **بوابات صلبة**: جلسة غير مفوضة، بيانات مقيدة، تحدي مصادقة، أو محول غير صحي كلها أسباب تمنع الإرسال مهما كانت الجودة المتوقعة.

5.3 سجل قدرات زمني

لا تُعامل أسماء النماذج وقدراتها كحقائق ثابتة. يحتفظ Web Model Capability Registry بملاحظات مؤرخة: نوع المهام، اللغات، الاستشهادات، الملفات، طول السياق الظاهر، أنماط البحث، وسجل الأخطاء. ويفصل بين الوسم الظاهر وبين تخمين النموذج الخلفي. تنتهي صلاحية الادعاءات عند تغير الواجهة أو السياسة أو عند تجاوز مدة المراجعة.

5.4 التوجيه متعدد اللوحات

يفتح النظام لوحة ثانية في ثلاث حالات: وجود خلاف متوقع بين النماذج؛ حساسية القرار للحقيقة؛ أو طلب مقارنة صريح. لا يقاس التوافق بتشابه الأسلوب، بل بتحليل ادعاءات ذرية: كيان، علاقة، تاريخ، كمية، شرط، درجة ثقة. وإذا استمر التعارض ينتقل المسار إلى مصادر أولية أو مراجعة بشرية بدل التصويت البلاغي.

جدول 2 - سياسة التوجيه بحسب نوع المهمة

نوع المهمة	المسار المفضل	عدد اللوحات	بوابة القبول
صياغة/إبداع منخفض المخاطر	محلي أو لوحة واحدة	1	الالتزام والملاءمة
بحث حديث	مصادر أولية + نموذج مساعد	1-2	الاستشهاد والحداثة
برمجة	بيئة محلية + نموذج مختص	1	اختبارات قابلة للتنفيذ
قرار عالي المخاطر	مصادر موثوقة + إنسان	0-2	لا اعتماد منفرد على نموذج ويب

مقارنة نماذج	أغلفة متكافئة	2-3	مقارنة ادعاءات لا أساليب

5.5 التراجع المشروع

إذا ظهر حد سرعة، ينتظر النظام وفق الإشارة الظاهرة ويستهلك ميزانية إعادة محدودة. يمكن الانتقال إلى خدمة أخرى فقط إذا كانت معتمدة ومناسبة، لا بقصد الالتفاف على قيد الحساب الأول. هذا الفرق بين **Fallback شرعي** و**Quota Evasion** جزء من منطق التوجيه نفسه، لا تحذير خارجي.

6. التحكم الكامل في المتصفح والجلسات

6.1 معنى «الواجهة الكاملة»

يشمل التحكم الكامل خمس مناطق: محتوى الصفحة، وشريط المتصفح والتبويبات، والحوارات الأصلية، وإدارة الملفات، وحالات الاستيلاء البشري. لا يعني ذلك أن كل متصفح يكشف القدرات نفسها؛ لذلك تُستبدل دعوى «كل المتصفحات» بمبدأ **التغطية المتدرجة**: دعم أولي لمحركات معروفة، دعم مشروط لمشتقات Chromium، ثم جسر UIA لأي تطبيق يكشف شجرة إتاحة كافية.

6.2 أنماط الجلسة

- **isolated_ephemeral:** جلسة مؤقتة للصفحات العامة، لا كتابة دائمة لبيانات التصفح.
- **dedicated_persistent:** ملف مخصص لخدمة وحساب وثقة محددة، وهو النمط المفضل للوحات المصرح بها.
- **attach_existing:** الاتصال بتبويب يفتحه المستخدم؛ أعلى خطرًا لأنه قد يكشف جلسات غير مرتبطة بالمهمة.
- **manual_takeover:** نقل التحكم للمستخدم عند الدخول أو MFA أو CAPTCHA أو الموافقة أو الدفع.

تدعم BrowserContexts العزل بين الجلسات [2]، لكن الاستفادة الآمنة منها تقتضي ألا يُعاد استعمال storage state خارج حد الثقة. كما أن الملفات الدائمة ينبغي أن تكون منفصلة عن الملف الشخصي الأساسي؛ ويؤكد تشدد Chrome في تصحيح الجلسة الافتراضية أهمية هذا الفصل [6].

6.3 إدارة النوافذ والتبويبات

يربط Cross-Browser Tab and Window Governance كل صفحة بـtask_id وadapter_id وorigin. إذا فتحت الخدمة تبويبًا جديدًا ينتظر النظام حدث الصفحة قبل النقر، ويُسجل الأب والابن. أي نافذة بلا أصل متوقع تعامل كـorphan وتُجمّد حتى المراجعة. وتغلق التبويبات ضمن سياسة الاحتفاظ، بدل ترك سجل معرفي مفتوح في المتصفح.

6.4 الحوارات والملفات

تتحقق طبقة UIA من أن الحوار تابع لعملية المتصفح المقصودة قبل اختيار ملف أو تأكيد حفظ. لا يُسمح بتصفح نظام الملفات بحرية؛ بل تعتمد **Upload Allowlist** ومجلد تنزيل معزول. يُعرض اسم الملف وحجمه وبصمته قبل الرفع، وتُحجر التنزيلات ولا تُنفذ آليًا. أما نوافذ كلمات المرور أو التصاريح القانونية فتعاد فورًا للإنسان.

6.5 اكتشاف الاكتمال

لا يستخدم النظام زمن انتظار ثابتًا وحده. يراقب اختفاء زر الإيقاف، واستقرار النص لعدة ثوان، ووجود حاوية الرسالة النهائية، وانتهاء ظهور الروابط أو المرفقات، وغياب «استمر في التوليد»، وعدم ظهور خطأ أو تسجيل دخول. يُطلب نصاب من ثلاث إشارات على الأقل بينها استقرار النص. هذا يمنع التقاط نصف إجابة أو إعادة حقن مخرجات قبل اكتمالها.

> **حالة الاكتمال:** auth_required | rate_limited | error | challenge | partial | complete. لكل حالة مسار تعافٍ مختلف؛ ولا تتحول partial إلى complete بالتخمين.

7. منظومة الأربعين HyperSkills

7.1 من قائمة مهارات إلى جهاز معرفي

تُعرّف HyperSkill هنا كوحدة تشغيل تحتوي محفزاً، ومدخلات، وشروطًا قبلية، وإجراءً، ومخرجات، وحالات فشل، ومقاييس، وروابط بمهارات أخرى. لا تُحمّل الأربعون كلها في كل مهمة؛ بل يسترجع الوكيل ما يلزم حسب مرحلة الحلقة، محققًا اقتصاد السياق وتخصص السلوك.

ب. التوجيه والتعبئة (HS-09..16)

تصنيف المهمة، سجل قدرات النماذج، بوابة التفويض والحصص، بناء QueryEnvelope، حماية نزاهة الPrompt، اختيار المحول، تسلسل التفاعل، وكشف الاكتمال متعدد الإشارات.

أ. الإدراك والتحكم (HS-01..08)

اكتشاف متصفحات Windows، بصمة القدرات، عزل الجلسة، لقطة الإتاحة، حل الهدف الدلالي، التأريض البصري الاحتياطي، جسر الحوارات الأصلية، وحوكمة التبويبات.

د. الجودة والذاكرة (HS-24..28)

تقييم MCD، محكمة الهدم والفجوات، ضغط السياق، إعادة الحقن في حالة الهدف، والكتابة إلى الذاكرة بوابات دليل.

ج. الاستخراج والدليل (HS-17..23)

التقاط البث، استخراج البنية، سلسلة المنشأ، التطبيع المحافظ، حفظ الروابط، كشف التعارض الزمني، والإجماع المحدود بين اللوحات.

و. المرونة والتحقق (HS-34..40)

كشف انجراف UI، التعافي والRollback، إعادة التشغيل التدقيقية، Sandboxing، دفاع Prompt Injection، تحقق الأثر العالمي، وإعادة البناء المحكومة.

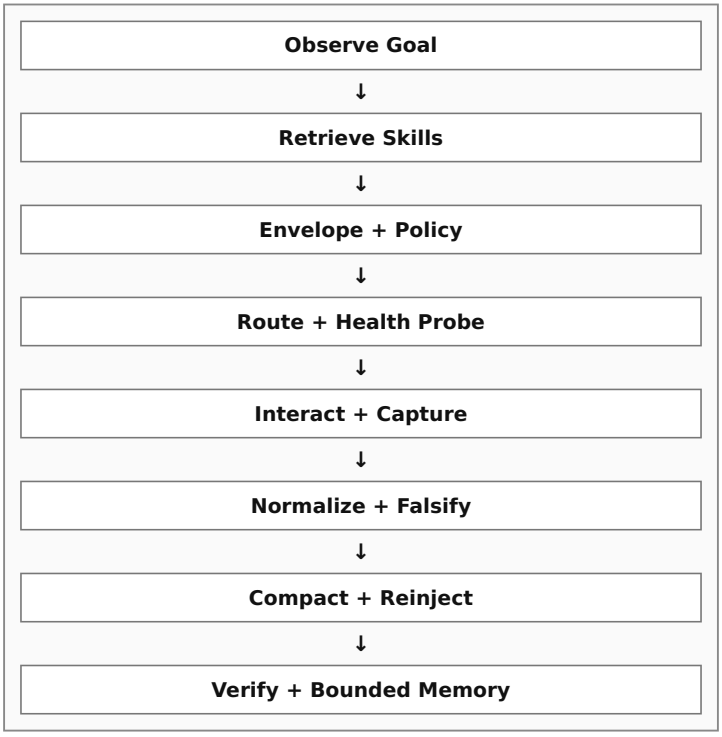
هـ. الأمن والحوكمة (HS-29..33)

حدود الاعتماد، تنقيح الأسرار وPII، مراجعة الشروط والموافقة، الاستيلاء البشري لتحديات المصادقة، والتراجع عند حدود السرعة.

7.2 ترابط المهارات

تظهر القوة من العلاقات لا من العدد. فHS-12 يثبت الحاوية، وHS-13 يقيس تغير النص، وHS-19 يربط البصمات، ثم HS-25 يختبر النتيجة وHS-27 يعيدها إلى الهدف. وبالمثل يوقف HS-34 المحول عند انجراف حرج، ويولد HS-40 رقعة مقترحة، لكن لا ينشرها حتى تمر باختبارات dry-run ومراجعة بشرية ونسخة قابلة للرجوع.

7.3 حلقة التشغيل المعيارية



7.4 حدود الحلقة

المهمة العادية: مسار واحد وإعادة واحدة. المهمة المركبة: مساران وبحد أقصى محاولتان إجماليتان. أما المهام عالية المخاطر فلا تعتمد ناتج نموذج ويب بوصفه الدليل الرئيسي. هذه الحدود تمنع تحول «المزيد من التفكير» إلى تكرار مكلف أو تضخيم للخطأ.

8. الاستخراج والمنشأ وإعادة الحقن

8.1 سلسلة الدليل

يُحفظ لكل نتيجة: نص الطلب الدقيق، وبصمته، والأصل، واسم الخدمة، والوسم الظاهر للنموذج، وإصدار المحول والمتصفح، ووقت البداية والنهاية، والنص الخام، والروابط، وأحداث الإعادة والخطأ. ترتبط الأحداث ببصمة الأب لتكوين سجل قابل لاكتشاف العبث، مع استبعاد ملفات الارتباط والرموز السرية.

8.2 التطبيع دون التملك

التطبيع عملية شكلية: إزالة شريط الأدوات، وتوحيد المسافات، وحفظ العناوين والقوائم والكود والجداول. لا يسمح للمطبع أن يضيف تفسيرًا أو يحذف تحذيرًا أو يقلب نفيًا. وإذا تعذر تمثيل جدول معقد، يُرفق تحذير بدل إخراج نص يبدو كاملًا وهو فاقد للبنية.

8.3 محكمة الهدم

تحلل المحكمة النتيجة وفق: الالتزام بالتعليمات، الاكتمال، الاتساق الداخلي، دعم الأدلة، سلامة الاستشهاد، الحداثة، قابلية الفعل، والامتثال. وتستخرج الادعاءات الحرجة ثم تسأل: ما الدليل المطلوب؟ هل الرابط يثبت الادعاء؟ هل توجد قفزة من وصف إلى حكم؟ هل أهمل قيدًا من السؤال؟ هل التاريخ متوافق مع زمن المهمة؟

$$\textbf{Accept} \Leftrightarrow A \geq .75 \wedge C \geq .70 \wedge I \geq .75 \wedge \text{Safety}=1 \wedge \text{CriticalUnsupported}=0$$

هذه العتبات مرجعية قابلة للمعايرة. وفي المجالات الطبية والقانونية والمالية لا تكفي النتيجة ولو تجاوزتها؛ بل تتحول إلى مدخل ثانوي لمصدر أولي أو مختص.

8.4 الضغط السياقي

لا يُلقى سجل المحادثة كاملًا في ذاكرة الوكيل. يحتفظ المخزن بالنص الخام، بينما تدخل إلى السياق حزمة مركزة تضم: هوية النتيجة، أهم الادعاءات، الأدلة، التعارضات، الأسئلة المفتوحة، والفعل التالي. يجب أن يحفظ الضغط الأرقام، والتواريخ، والشروط، والنفي، وعدم اليقين. ويقاس نجاحه بقدرته على إعادة بناء القرار، لا بعدد الرموز المحذوفة.

8.5 إعادة الحقن الموثق

```
[EXTERNAL_MODEL_OBSERVATION]
Source: service / visible-model-label
Prompt hash: ...
Confidence: 0.82
Claims: ...
Evidence: ...
Contradictions: ...
Limitations: ...
Recommended use: corroborate | transform | reject | human-review
[/EXTERNAL_MODEL_OBSERVATION]
```

تمنع الوسوم الخلط بين أربعة أصناف: حقائق صرح بها المستخدم، وأدلة أدوات، وادعاءات نموذج خارجي، واستنتاجات الوكيل. هذا الفصل هو لب «إعادة الحقن»: النتيجة تغير خطة الهدف عبر قناة معلنة، لا عبر اندماج لغوي خفي.

8.6 الذاكرة ثلاثية الطبقات

Task Store للنص الخام المؤقت، **Evidence Store** للادعاءات المتحققة، **Skill Memory** لدروس المحولات والانجراف. لا يصبح الادعاء دائمًا إلا مع منشأ، وملاءمة، وسماح احتفاظ، وثقة تحقق. أما إصلاحات المحولات فلا تصبح مهارة إلا بعد إعادة تشغيل ناجحة ومراجعة.

9. الأمن والحوكمة ومقاومة الحقن

9.1 المتصفح كسطح هجوم معرفي

عندما يقرأ الوكيل صفحة ثم يمتلك أدوات، يمكن لنص الصفحة أن يحاول تحويل نفسه من «بيانات» إلى «أوامر». تصف OWASP حقن الـPrompt بأنه إدخال يغير سلوك النموذج بسبب ضعف الفصل بين التعليمات والبيانات [9]، وتوصي إرشادات أمن الوكلاء بمعاملة كل البيانات الخارجية بوصفها غير موثوقة، وبفرض حدود امتياز واضحة [10]. لذلك لا تمنح SWRM الصفحة سلطة؛ السلطة محفوظة للحاوية والسياسة.

9.2 دستور الأتمتة

1. العمل في حسابات وجلسات وبيانات مخول بها فقط.
2. عدم تجاوز CAPTCHA أو MFA أو الدفع أو الحصص أو ضوابط المنصة.
3. عدم تدوير الحسابات أو إخفاء البصمة بقصد تفادي الكشف أو الحدود.
4. منع الأسرار وملفات الارتباط وقواعد كلمات المرور من دخول السجلات أو السياق.

5. اعتبار النشر والإرسال والشراء والحذف أفعالًا مستقلة تحتاج موافقة.
6. جعل dry-run وreview_required افتراضيين للمحول الجديد أو المتغير.

9.3 تصنيف البيانات

الصنف	سياسة الويب	الاحتفاظ
Public	خدمات معتمدة	Task-only افتراضيًا
Internal	خدمة مصرح بها صراحة	وفق الحاجة
Confidential	محلي افتراضيًا، موافقة لكل مهمة	حد أدنى
Restricted	ممنوع على لوحات خارجية	محلي فقط

9.4 كشف التعليمات الخبيثة

تُراجع الصفحة والنتيجة بحثًا عن أوامر تطلب كشف أسرار، أو تعطيل السياسة، أو تشغيل أوامر محلية، أو الانتقال إلى أصل جديد، أو تحميل ملف وتنفيذه، أو تغيير الهدف. تحفظ هذه النصوص كأدلة مقتبسة ولا تنفذ. وفي حالة الشك ينتقل النظام إلى محكمة الحقن أو المراجعة البشرية.

9.5 الحوكمة وفق إدارة المخاطر

يتوافق التصميم مع منطق إدارة المخاطر في NIST AI RMF الذي ينظم العمل حول الحوكمة، والخريطة، والقياس، والإدارة [11]، ومع ملف المخاطر للذكاء التوليدي [12]. في SWRM: **Govern** هو الدستور وسجل الشروط؛ **Map** تصنيف المهمة والبيانات؛ **Measure** مقاييس النزاهة والانجراف؛ و**Manage** الإيقاف، والتراجع، والموافقة، والذاكرة المقيدة.

> **قاعدة الأثر:** كل فعل يغير العالم يجب أن يمتلك حالة قبلية متوقعة، وفعلًا واحدًا محدودًا، وملاحظة بعدية مستقلة، وقرار نجاح/فشل/التباس.

10. منهجية التقييم والتجارب المقترحة

10.1 أسئلة التقييم

يقيم البرنامج التجريبي النظام لا النموذج الخارجي فقط. الأسئلة: هل ينقل الطلب دون تحريف؟ هل يميز الاكتمال؟ هل يحفظ الاستشهادات؟ هل يمنع تسرب الجلسة؟ هل يتعافى من تغير الواجهة؟ هل يقلل محكمة الهدم من الادعاءات غير المدعومة؟ وهل تحسن إعادة الحقن أداء الوكيل النهائي مقارنة بلصق النص الخام؟

10.2 مجموعة الاختبار

تُبنى مجموعة من 240 مهمة موزعة بالتساوي على: بحث حديث، تحليل مركب، برمجة، تلخيص طويل، استخراج من ملفات، ومقارنة نماذج. تنفذ على Chromium وEdge وFirefox، ومع محولين تجريبيين على الأقل لكل صنف يسمح به الاستخدام. تُكرر كل مهمة في ثلاثة أوضاع: **نسخ يدوي، أتمتة واجهة غير محكومة، و SWRM.**

10.3 المقاييس

المقياس	التعريف	الهدف الأولي
Prompt Fidelity	تطابق النص المرسل مع الحاوية	≥ 0.995
Completion Precision	نسبة حالات complete الصحيحة	≥ 0.97
Capture Integrity	حفظ النص النهائي بلا فقد/تكرار	≥ 0.98
Citation Preservation	الروابط والوسوم الصحيحة	≥ 0.95
Session Isolation	غياب تسرب حالة بين المهام	1.00
Injection Containment	تعليمات الصفحة غير المنفذة	≤ 0.99
Reinjection Utility	تحسن نجاح الوكيل النهائي	+15% نسبي
Drift Recovery Time	من الكشف إلى رقعة مراجعة	يُخفض عبر الإصدارات

10.4 تجارب الإزالة Ablation

- إزالة بصمة الـPrompt لقياس أثرها في اكتشاف التحريف.
- استبدال كشف الاكتمال المتعدد بانتظار ثابت.
- إعادة حقن النص الخام بدل الحزمة الموسومة.
- إلغاء عزل BrowserContext.
- إلغاء محكمة الهدم أو الاستشهادات.
- استخدام عدة لوحات افتراضيًا بدل التوجيه الندري.

تسمح هذه التجارب بإسناد الفائدة إلى مكونات محددة بدل تقييم الحزمة ككتلة واحدة. المتوقع أن تكون أكبر خسارة في السلامة من إلغاء العزل، وأكبر خسارة معرفية من إلغاء المحكمة والوسم، وأكبر خسارة في الاستقرار من انتظار ثابت أو ربط المنطق بالمحددات مباشرة.

10.5 اختبار انجراف الواجهة

يولد المختبر نسخًا متغيرة من واجهة تجريبية: تغيير أسماء داخلية، نقل الأزرار، تبديل البث، إضافة نافذة موافقة، فتح الرد في تبويب، أو تغيير بنية الاستشهادات. يقاس هل تفشل المهارة بأمان، وهل تمنع الإرسال عند الغموض، وهل تنتج حزمة إصلاح مصغرة. النجاح ليس استمرار النقر بأي ثمن؛ بل **التوقف الصحيح** عند غياب اليقين.

10.6 قابلية التكرار

يحفظ الإصدار، والبصمات، والعقود، وصور الإتاحة، ونتائج الاختبارات دون أسرار. وتعاد التجربة في ملف جديد، لأن تكرار جلسة المستخدم قد يخلط أثر النظام بأثر سجل شخصي. كما يُفصل زمن النموذج عن زمن التحكم كي لا يُنسب بطء الخدمة إلى المحول.

11. المناقشة والحدود وخارطة التطوير

11.1 القيمة العلمية والهندسية

تنقل المعمارية النقاش من «هل يستطيع الوكيل النقر في Chat UI؟» إلى «تحت أي عقد معرفي وسياسي تصبح النتيجة قابلة للاستخدام؟». أهم ابتكار ليس مشغل المتصفح، بل **تحويل الواجهة إلى منفذ قدرة محدود الصلاحية**. فالنموذج الخارجي لا يلتحق بالعقل الوكيل مباشرة، بل يمر عبر وسيط يحافظ على هوية السؤال، ويقيس منشأ الجواب، ويحول المخرجات إلى ادعاءات قابلة للاعتراض.

11.2 لماذا لا يعوض API؟

يظل API أفضل عندما يتوافر تعاقد رسمي، ومخططات ثابتة، ومراقبة استخدام، وسجلات أخطاء، وسعة وتوافر محددان. أما مسار الويب فيضيف اعتمادًا على العرض، وعلى حالة الحساب، وعلى تغيرات غير معلنة. ولذلك يجب وصفه **بمسار قدرة تكميلي**؛ يصلح للوضع اليدوي-المحكوم، أو الميزات الويب-أول، أو المقارنات، أو التجارب، لا كبنية تحتية وحيدة لخدمة حرجة.

11.3 حدود البحث

- الورقة تقدم معمارية وبرنامج تقييم، ولا تدعي نتائج تجريبية نهائية قبل تنفيذ Benchmark متعدد الخدمات.
- إمكانية التحكم تعتمد على ما تكشفه الصفحة والمتصفح وشجرة الإتاحة.
- شروط الخدمات متغيرة ويجب مراجعتها لكل محول وزمن استخدام.
- لا توجد آلية كاملة لمنع Prompt Injection؛ الدفاع طبقي واحتمالي [9][10].
- الوسم الظاهر للنموذج قد لا يثبت البنية الخلفية الحقيقية.
- الضغط السياقي قد يسقط تفاصيل؛ لذلك يبقى النص الخام في سجل محدود.

11.4 خارطة التطوير

1. **SWRM-Bench:** مجموعة قياس مفتوحة للواجهات التجريبية والانجراف.
2. **Adapter DSL:** لغة وصف تصريحية للأصول، والعناصر، وإشارات الاكتمال، والحوكمة.
3. **Semantic Snapshot Diff:** مقارنة شجرة الإتاحة بدل صور البكسل فقط.
4. **Claim Graph Reinjection:** تمثيل النتيجة كشبكة ادعاءات وأدلة وتعارضات.
5. **Cross-Model Evidence Arbitration:** محكمة تميز اتفاقًا مستقلًا من تكرار مصدر واحد.
6. **Formal Policy Proofs:** اختبار أن مسارات الأفعال لا تتجاوز وضع الموافقة المحدد.

7. **Hermes/Codex Bridges:** عقود أدوات منفصلة للقراءة، والتعبئة، والإرسال، والتحقق.

11.5 النتيجة النظرية

يمكن القول إن المتصفح يصبح جزءًا من معمارية AGI-oriented فقط عندما يخضع لمنطق حاكمي أعلى من الصفحة والنموذج معًا. فلو كانت الواجهة هي التي تحدد ما يفعله الوكيل، ضاع الهدف. ولو كان النموذج الخارجي هو الذي يحدد ما يصدق، ضاع الدليل. ولو كانت الذاكرة تقبل كل نص، ضاعت الهوية المعرفية. السيادة هنا هي إبقاء الهدف والسياسة والمنشأ والتحقق أعلى من القدرة المستعملة.

11.6 الهندسة المعرفية الشاملة للوكيل

تقوم الهندسة المعرفية المقترحة على التمييز بين **ذكاء الخدمة وذكاء الوكيل**. ذكاء الخدمة هو القدرة المحلية للنموذج الخارجي على البحث أو البرمجة أو التحليل؛ أما ذكاء الوكيل فهو القدرة الأعلى على تحديد متى تُستدعى هذه الخدمة، وما الذي يُرسل إليها، وكيف يُفهم جوابها، وما الذي يُحتفظ به منها. إذا ذاب المستويان صار الوكيل تابعًا لبلاغة آخر نموذج استُدعي. وإذا فُصلا صار تعدد النماذج سوق قدرات يخضع لهدف واحد وذاكرة واحدة ومحكمة واحدة.

لهذا تُقسم دورة المعرفة إلى سبع حالات: حاجة غير محلولة، ثم فرضية توجيه، ثم طلب ثابت، ثم مشاهدة خارجية، ثم ادعاءات مفككة، ثم دليل متحقق، ثم تغيير في خطة الهدف. لا يجوز القفز من الطلب إلى تغيير الخطة؛ إذ تقع بينهما طبقات المنشأ والهدم والضغط. وتسمح هذه الحالات للوكيل بتحديد سبب امتلاكه لكل معلومة، وما إذا كانت تحتاج إلى تجديد، وما إذا كان اختلاف نموذج جديد ينقضها أو يوسعها.

وتُبنى الذاكرة فوق **مفاتيح معرفية** لا فوق المحادثات فقط: مفتاح الادعاء، ومفتاح الدليل، ومفتاح الزمن، ومفتاح الحساسية، ومفتاح المهمة التي أنتجته. بهذه الطريقة يمكن حذف سجل جلسة خاصة مع إبقاء نتيجة عامة متحققة، أو إسقاط ادعاء قديم مع حفظ تاريخ اتخاذ القرار، أو إعادة تشغيل المسار عند تغير واجهة أو نموذج دون خلط النسخة الجديدة بالقديمة.

11.7 موقع SWRM بين RPA وAPI وMCP

المقاربة	نقطة القوة	الحد البنيوي	دور SWRM
RPA التقليدي	تنفيذ إجراءات واجهة متكررة	ضعف تمثيل الدليل والهدف المعرفي	يضيف الحاوية والمحكمة وإعادة الحقن
API	عقد ثابت ومخرجات منظمة	قد لا يغطي قدرات Web-first أو الحساب اليدوي	يبقى المسار المفضل حين يتوافر ويُستخدم نكحط مقارنة
MCP / Tools	فصل الأدوات بعقود قابلة للاكتشاف	يحتاج أداة خلفية أو محولًا للواجهة	يقدم مجموعة أدوات Browser-side محكومة
نسخ يدوي	وضوح تدخل الإنسان	فقد المنشأ والتكرار والقياس	يحافظ على المراجعة البشرية مع سجل منظم

لا تنافس SWRM هذه المقاربات جميعًا، بل تنظم العلاقة بينها: تفضّل API أو Connector عندما يكون رسميًا وملائمًا؛ تستعمل MCP لتقديم الوظائف إلى الوكيل؛ وتستعمل التحكم الرسومي فقط عندما يكون هو المنفذ المشروع أو الأكثر فائدة. وبذلك يصبح المتصفح جزءًا من بنية متعددة القنوات بدل أن يتحول إلى بديل أعمى لكل تكامل.

«لا يكون Web Console عقلًا ثانيًا للوكيل، بل عضوًا معرفيًا خارجيًا محدود الصلاحية، لا تُقبل إفادته إلا ببصمة، ومنشأ، ومحكمة، وأثر قابل للرجوع.» - زهير مساعف

---

12. الخلاصة والمراجع

12.1 الخلاصة

قدمت الورقة SWRM كمعمارية KB-as-OS تستعمل المتصفح ناقلًا محكومًا لقدرات الذكاء الاصطناعي المتاحة عبر الويب. تقوم المعمارية على فصل جوهر المهمة عن محول الخدمة، وعلى توجيه ندري يسبق الجودة فيه التفويض والسياسة، وعلى تحكم دلالي قبل التحكم البصري، وعلى كشف اكتمال متعدد الإشارات، وعلى حفظ النص الخام والمنشأ، وعلى محكمة هدم قبل إعادة الحقن، وعلى ذاكرة لا تقبل إلا المعرفة المتحققة.

لا يتحقق التقارب مع API بمحاكاة شكل الطلب والجواب، بل ببناء **حاوية تشغيلية** تحافظ على النزاهة والتفسير والحدود. ومن ثم فإن مساهمة المشروع ليست طريقة للحصول على خدمات قوية دون API، بل هندسة تجعل استعمال الواجهة - حين يكون مشروعًا ومناسبًا - قابلًا للإدماج في حلقة Agentic دون أن تصبح هشاشة الصفحة أو بلاغة النموذج سلطة على العقل.

يؤسس ذلك لمسار بحثي أوسع: الوكيل العام لن يعيش داخل نموذج واحد أو API واحد، بل سيحتاج إلى اختيار قدرات خارجية، وإدارة سياقاتها، والتحقق من مخرجاتها، وإعادة تركيبها ضمن هدفه. SWRM تقدم نموذجًا أوليًا لهذه الحاكمية: **الوصول قبل الاستعمال، الدليل قبل الذاكرة، والتحقق قبل الأثر.**

12.2 الملخص الشامل المحيط

يمكن اختزال الهندسة المعرفية الكلية في خمس طبقات متعاقبة. طبقة **الحاكمية** تحدد ما يجوز فعله، وبأي حساب، ومع أي صنف بيانات. طبقة **التعيين** تحول الهدف إلى حاوية قابلة للقياس وتختار أقل طريق كاف. طبقة **التفاعل** تنفذ عبر دلالات الواجهة مع عزل الجلسة والتوقف عند الغموض. طبقة **الدليل** تحفظ النص الخام والمنشأ والتوقيت والاستشهادات. وأخيرًا طبقة **الاستيعاب** تفكك المخرج إلى ادعاءات، وتمرره بمحكمة الهدم، ثم تعيده إلى حالة الهدف في صورة ملاحظة موسومة. إن فقدان طبقة واحدة يحول النظام من وكيل محكوم إلى سلسلة نقرات أو إلى ذاكرة تستقبل نصوصا بلا معيار.

ضمن مشروع MOUSSAIF9B، تعمل SWRM كجهاز وصل بين النواة المعرفية وفضاء نماذج الويب. النواة لا تتنازل عن هدفها أو سياستها للنموذج الخارجي؛ بل تستدعيه كقدرة مؤقتة، وتعيد بناء فائدته داخل خرائط الأدلة والأسئلة المفتوحة. وبذلك يصبح اختلاف مزودي النماذج وتغير واجهاتهم مصدر تنوع يمكن توجيهه بدل أن يكون سببا لتفتت الذاكرة أو ازدواج التعليمات.

12.3 مصفوفة الإسهام والتحقق

الإسهام	الأثر المتوقع	دليل القياس
الترحيل السيادي	منع اعتماد قدرة غير مفوضة أو نتيجة بلا منشأ	Authorization + Provenance pass rate
استقلال الجوهر عن الواجهة	خفض كلفة تغير UI وحصر الإصلاح في Adapter	Drift repair time + regression success
التكافؤ التشغيلي المقيد	مقارنة منضبطة مع API دون ادعاء التطابق	Qop vector and failure decomposition
إعادة الدخول السياقي	منع تحول جواب خارجي إلى سلطة غير موسومة	Claim attribution + reinjection utility
الندرة التوجيهية	خفض الإفصاح والكلفة والتعارض غير الضروري	Consoles per task + marginal quality gain

القرار التنفيذي: يبدأ النشر بمتصفح واحد وAdapter واحد لمهام عامة منخفضة الحساسية، مع إرسال يدوي ومراقبة كاملة. لا ينتقل المحول إلى التشغيل شبه الآلي إلا بعد اجتياز اختبارات النزاهة والانجراف والحقن. ولا تنتقل أي مهمة إلى أفعال مؤثرة إلا عبر أداة منفصلة وموافقة صريحة وتحقق من الأثر. هذه المراحل تجعل التوسع تراكما في الثقة، لا توسعا في الصلاحيات.

12.4 برنامج التنفيذ المرحلي

يقترح التطبيق أربع مراحل. في **مرحلة الإثبات** تُختار مهام عامة وخدمة واحدة، ويظل الإرسال يدويًا، بينما يقيس النظام التعبئة والالتقاط والمنشأ. في **مرحلة الثقة** تُضاف اختبارات الانجراف والحقن والملفات، وتعاير عتبات الاكتمال والجودة. في **مرحلة الوكالة** يسمح بالتوجيه الآلي للقراءة والتحليل فقط، مع بقاء الأفعال المؤثرة منفصلة. وفي **مرحلة التوسع** تضاف متصفحات وخدمات ومجالات جديدة بعد مراجعة كل حد ثقة، لا بنسخ محول واحد على الجميع.

ينبغي أن يكون معيار الترقية هو انخفاض الغموض لا زيادة عدد المهام. المحول الناضج هو الذي يعرف متى يتوقف، ويحفظ ما فشل في فهمه، ويتيح إعادة التشغيل، ولا يربط النجاح باستمرار النقر. ومن ثم تصبح مؤشرات مثل صحة الإيقاف، ودقة نسبة الادعاء إلى مصدره، وصفر تسرب للأسرار أهم من معدل إكمال ظاهري مرتفع.

12.5 قواعد الاعتماد النهائي

يُقترح اعتماد ست قواعد غير قابلة للتجاوز في أي نشر فعلي: **قاعدة الأصل**، فلا تفاعل خارج قائمة الأصول المسموحة؛ **قاعدة الهوية**، فلا حساب أو ملف جلسة بلا مالك وحد ثقة معروف؛ **قاعدة النص**، فلا إرسال من دون نسخة ثابتة وبصمة؛ **قاعدة الاكتمال**، فلا التقاط بناء على الزمن وحده؛ **قاعدة المعرفة**، فلا ذاكرة دائمة قبل التحقق والمنشأ؛ **وقاعدة الأثر**، فلا فعل خارجي بلا موافقة وتحقق بعدي. تمثل هذه القواعد الحد الأدنى الذي يحول النظام من Browser Bot إلى بنية Agentic مسؤولة.

وتبقى الجودة المقاربة للAPI نتيجة تراكم هذه الضمانات، لا خاصية منفردة في أداة التحكم. قد ينجح محدد العنصر مئة مرة، لكن المسار يظل ضعيفًا إن لم يثبت أي حساب استُعمل أو إن لم يحفظ نص السؤال أو إن خلط جواب النموذج بحقيقة المستخدم. وبالعكس، يمكن لمسار أبطأ يحتاج مراجعة بشرية أن يكون أعلى قيمة عندما يضمن سلامة التفويض والدليل. لذلك ينبغي أن تعرض لوحة التشغيل متجه الجودة كاملا، لا رقم نجاح واحدا يخفي موضع الضعف.

معيار النضج: لا يقاس النظام بعدد المواقع التي يستطيع تشغيلها، بل بعدد الحالات التي يستطيع فيها تفسير قراره، والتوقف بأمان، وإعادة بناء الدليل، ومنع النتيجة غير المتحققة من تغيير الهدف.

المراجع

1. Microsoft Playwright. *Browsers*: *Chromium, WebKit, Firefox, Google Chrome and Microsoft Edge*. Official Documentation, accessed July 2026.
2. Microsoft Playwright. *Isolation and Browser Contexts*. Official Documentation, accessed July 2026.
3. Microsoft Playwright. *Page Object Models*. Official Documentation, accessed July 2026.
4. Microsoft. *UI Automation for Win32 Applications*. Microsoft Learn, updated 2025.
5. Chromium Project. *Chrome DevTools Protocol*. Official Protocol Documentation, accessed July 2026.
6. Google Chrome Developers. *Changes to Remote Debugging Switches to Improve Security*, March 2025.
7. W3C. *WebDriver*. W3C Technical Report, July 2026.
8. W3C. *WebDriver BiDi*. W3C Working Draft, June 2026.
9. OWASP Cheat Sheet Series. *LLM Prompt Injection Prevention Cheat Sheet*, accessed July 2026.
10. OWASP Cheat Sheet Series. *AI Agent Security Cheat Sheet*, accessed July 2026.
11. Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1, 2023.
12. Autio, C. et al. *Artificial Intelligence Risk Management Framework*: *Generative AI Profile*. NIST AI 600-1, 2024.
13. Moussaif, Z. *Sovereign WebConsole Relay Mesh - MOUSSAIF9B Browser KB-as-OS, Master Specification v1.0*, 2026.
14. Google Chrome Developers. *chrome.debugger Extension API*. Official Documentation, updated 2026.
15. Microsoft Playwright. *Pages, Popups and Multiple Tabs*. Official Documentation, accessed July 2026.

توفر الأثر الهندسي: الحزمة المرجعية المصاحبة تتضمن Master KB-as-OS، وأربعين HyperSkills مستقلة، وعقود JSON، ومرجع Runtime، ومثبت PowerShell، وجسور Hermes/Codex، وسياسات أمن واسترجاع.