Umíme to ještě bez AI?

Co se může pokazit, i když to na první pohled funguje

Jiří Šlachta

AI modely v průmyslu: Transformace z různých pohledů | IT4I AI Factory Hub | 23. 10. 2026

Pondělí 8:15.

AI nejede.

Co udělá váš tým?

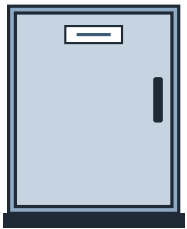
Problém není výpadek, ale co přijde po něm



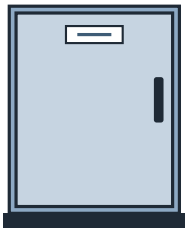
Tohle už není technologické riziko.

Je to provozní závislost.

Váš dodavatel už AI používá



Dodavatel A
rychle, levně, nějak funguje

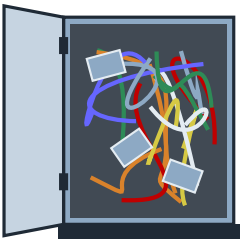


Dodavatel B
testované, doložitelné

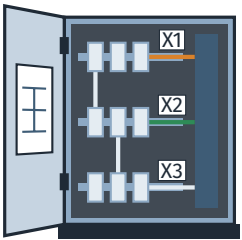
Při převzetí vypadají obě dodávky stejně.

NIS2 po vás chce vědět i to, co je za dvířky.

Váš dodavatel už AI používá



Dodavatel A
rychle, levně, nějak funguje

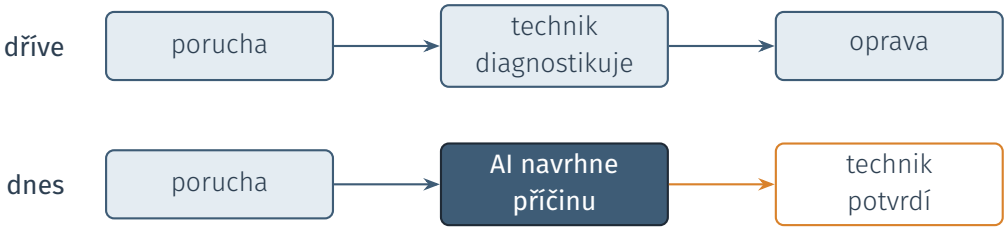


Dodavatel B
testované, doložitelné

Při převzetí vypadají obě dodávky stejně.

NIS2 po vás chce vědět i to, co je za dvířky.

Příklad 1: údržba



Člověk je pořád v procesu.

Jen se jeho role změnila z diagnostika na schvalovatele.

Problém není, že AI dělá chyby

AI může udělat chybu.

To jsme čekali.

Horší je, když postupně ztratíme lidi, kteří ji dokážou poznat.



Automatizace odstraní rutinu.

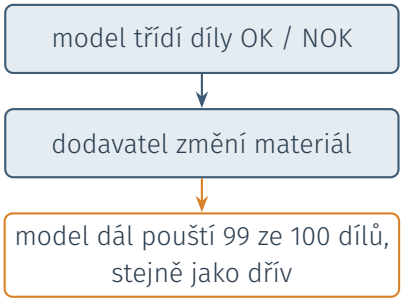
Člověku zůstanou výjimky.

A právě na výjimky přestane mít praxi.

Lisanne Bainbridge: *Ironies of Automation*, 1983

Budzyń a kol., *Lancet Gastroenterol Hepatol*, 2025: záchyt adenomů bez AI klesl po zavedení AI z 28,4 % na 22,4 %.

Příklad 2: vizuální kontrola kvality



O tři měsíce později

Reklamace od zákazníka.
Model se nemýlil hlasitě.
Mýlil se potichu a sebejistě.

Jak poznáte chybu, která vypadá jako správný výsledek?

Výpadek vs. tichá chyba

Výpadek
Model neodpovídá.
Ticket.
Incident.
Eskalace.

Tichá chyba
Model odpovídá.
Výstup vypadá dobře.
Nikdo si ničeho nevšimne.

Který problém má lepší monitoring?

Příklad 3: poskytovatel změnil model

Hlasitá změna	Tichá změna
Nový ceník.	Stará verze modelu končí.
Nové podmínky.	Nová má stejné API.
Regulace, export, region.	Odpovídá trochu jinak.
Přístup ztratíte a víte o tom.	**Nikdo to neotestoval.**

Model stále funguje. API stále funguje.

Jen už to není ten model, který jste ověřili.

Kam odcházejí vaše data?

Prompt

Výkresy, receptury, data zákazníků. Vše, co vložíte, opouští firmu.

Podmínky

Kde se data zpracovávají? Smí na nich poskytovatel trénovat?

Stínová AI

Co lidé používají mimo firemní nástroje, protože je to rychlejší?

Zákaz bez alternativy nefunguje.

Jen přesune AI tam, kde ji nevidíte.

Vlastní model jako řešení?

Méně závislosti na	Více závislosti na
ceníku a podmínkách poskytovatele	lidech, kteří model trénují a udržují
změnách verzí, které neřídíte	infrastruktuře a výpočetním výkonu
datech odcházejících ven	kvalitě vlastních dat

Závislost nezmizí.

Přesune se.

A co záložní řešení?



Existuje v dokumentaci?

To nestačí.

Kdy jste ho naposledy opravdu použili?

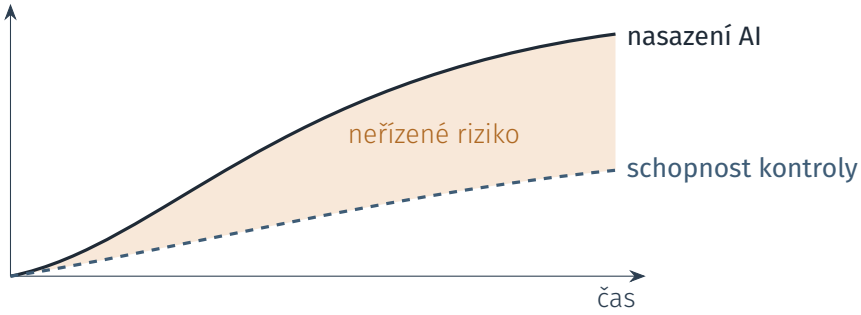
Tři rizika se navzájem posilují



Největší riziko není jedno z nich.

Je jejich smyčka.

Proč zpomalit



Zpomalit neznamená AI nezavádět.

Znamená nezavádět ji rychleji, než stíháte budovat kontrolu.

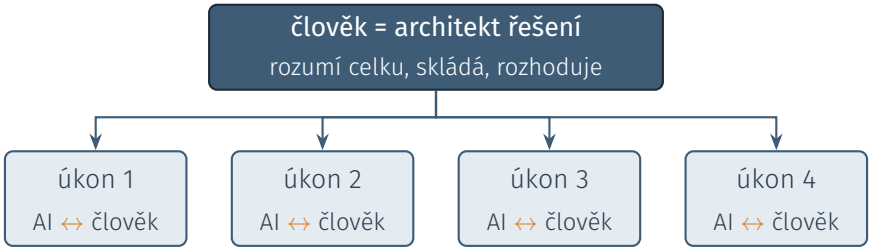
Co s tím: lidé a kontrola

- **Cvičte provoz bez AI.**
  Jako požární cvičení: pravidelně, naostro, s měřením, jak dlouho to trvá.
- **Měřte, jak často člověk AI opraví.**
  Pokud nikdy, kontrola nejspíš neprobíhá. Nula není dobrá zpráva.
- **Kontrolujte i výstupy, které vypadají dobře.**
  Namátkový vzorek, i když žádný alarm nehlásí problém.

Co s tím: modely, dodavatelé a data

- **Držte si referenční sadu případů.**
  Před každou změnou verze modelu ji projeďte a porovnejte výsledky.
- **Mějte plán odchodu.**
  Navrhněte práci tak, aby každý úkon, který dělá AI, uměl převzít člověk.
- **Určete, jaká data smí do které AI.**
  A dejte lidem schválený nástroj, ať nemusí hledat vlastní.

Plán odchodu začíná architekturou



AI pomáhá s atomickými úkony. Celek drží člověk.

Každý úkon jde vrátit člověku a ten ví, jak ho udělat.

Když AI zmizí, zpomalíte. Nezastavíte se.

Jeden dodavatel, dvě rychlosti



Tentýž vývojář. Pondělí: teplárna. Úterý: e-shop.

Dvourychlostní vývoj dlouho neudrží procesy ani lidé.

Rychlý režim často prosakuje do pomalého.

Platí i pro vás, pokud sami dodáváte do regulovaných odvětví.

Co už dnes řešíte

Rizika

Je AI ve vaší analýze rizik?

Dodavatelé

Je poskytovatel modelu mezi kritickými dodavateli? Víte, jak AI používají ostatní?

Kontinuita

Co uděláte, když AI zítra nebude?

AI nemusí vytvořit nový problém.

Může jen odhalit mezeru v tom, co už máte řídit.

Řízení rizik, dodavatelského řetězce a kontinuity činností: NIS2 a zákon o kybernetické bezpečnosti.

Tři otázky na zítřek

Kdo to u vás udělá bez AI?

Jak poznáte, že AI dělá chybu?

Co uděláte, když AI nebude?

Co nesmíme ztratit?

Co nesmíme ztratit?

schopnost rozhodnout, že AI nemá pravdu.