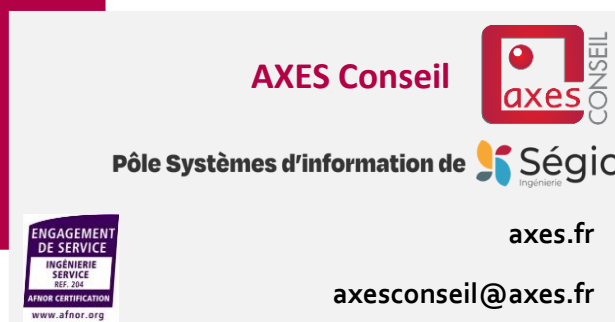


Interface MCP : Concilier des approches déterministes et probabilistes



L'un des champs d'application de l'IA générative (et agentique) dans la géomatique porte sur les modalités d'interaction avec l'outil SIG : l'utilisateur peut exprimer sa demande en langage naturel. La machine a la capacité d'interpréter cette demande puis exécuter l'opération.

Ce processus repose sur une brique centrale : le MCP (Model Context Protocol – publié en novembre 2024 par la société Anthropic – passage en standard et versé à la communauté fin 2025) qui joue un rôle d'interface entre le LLM et l'outil SIG. Cette technologie, déjà disponible sur QGIS ou ESRI, fait évoluer la notion d'interface entre machines.

Interagir en langage naturel avec un outil SIG

L'objectif est de demander au LLM, avec le support du MCP, de transformer une demande en langage naturel vers un texte structuré exploitable par une machine (serveur applicatif).

Quatre composants sont impliqués :

- Le moteur LLM,
- Le serveur MCP qui expose les fonctions exécutables sur l'outil SIG,
- Le client MCP qui assure la liaison entre le LLM et le serveur MCP,
- Le serveur ou composant applicatif sur lequel s'exécute les fonctions.

Le processus de principe est très schématiquement le suivant :

- Le client MCP récupère les descriptions des fonctions proposées par le serveur MCP et les met à disposition du LLM.

- Le LLM interprète la demande de l'utilisateur en langage naturel et identifie la ou les fonctions nécessaires.
- Le LLM génère un appel d'outil (Tool Calling) sous une forme structurée (par exemple en JSON).
- Le client MCP traduit le Tool Calling en une requête conforme au protocole MCP et la transmet au serveur MCP.
- Le serveur MCP appelle l'outil ou la fonction SIG correspondante.
- L'outil SIG exécute effectivement l'opération et retourne le résultat.

Illustration avec le MCP de l'IGN

Le test a pour objectif de répondre à la question « Quelle est l'altitude de telle montagne ? » en utilisant le MPC de L'IGN. Le LLM utilisé est la version de MISTRAL exécutée localement.

Pour répondre à cette question, deux fonctions, sur la dizaine de fonctions proposées par le MCP de l'IGN, sont à mobiliser :

- GEOCODE :
 - o Renvoie des résultats d'autocomplétion géocodés à partir d'un texte libre (lieu, adresse, POI), avec coordonnées, libellé complet et informations de localisation ('kind', 'city', 'zipcode'). Les coordonnées 'lon/lat' retournées sont directement réutilisables dans tous les autres tools. (Voir ci-dessous)
- ALTITUDE :
 - o Renvoie l'altitude (en mètres) et la précision de la mesure (accuracy) d'un point géographique à partir de sa longitude et de sa latitude.

Le LLM doit donc comprendre qu'il faut enchaîner deux actions :

- Identifier un toponyme dans la question en langage naturel pour obtenir ses coordonnées (lat/long)
- Obtenir l'altitude des coordonnées lat/long obtenues de la tâche précédente.

Le pseudo code du processus est donc :

leLieu := RécupérationDuLieuParLeLLM_ (« Altitude de la Meije ? »)

LesCoordonnées := GEOCODE (leLieu)

LaAltitude := ALTITUDE (LesCoordonnees)

Afficher 'L'altitude de' + leLieu + ' est de ' + LaAltitude + ' m'

Le LLM analyse la question et isole le toponyme. Il construit l'appel à l'outil GEOCODE (tool_calling) en passant en paramètre le toponyme (« Meije »).

Le service de l'IGN renvoie plusieurs toponymes « Meije ». Le nombre de toponymes renvoyés peut être paramétré.

Le LLM choisi une des valeurs en fonction des informations contenues dans la demande initiale et les informations portées par le service GEOCODE (« kind = Sommet » par exemple).

Ensuite, le LLM construit l'appel (tool_calling) correspondant à l'outil ALTITUDE, en utilisant les coordonnées géographiques fournies par le géocodeur. Le serveur MCP peut alors exécuter cet appel et retourner l'altitude correspondante.

Aux questions « Altitude du Mont Ventoux » et « Altitude du Ventoux », le LLM isole bien le terme VENTOUX mais ne fait pas le même choix dans la liste de toponymes proposés :

- A la première question, le LLM choisi un toponyme Mont Ventoux dont la valeur KIND = SOMMET.
- A la seconde question, le LLM choisi la commune de 01110 d'Aranc (01110), première valeur dans la liste dont la valeur KIND = SOMMET.

L'utilisation du terme HAUTEUR en remplacement de ALTITUDE donne des résultats différents :

- « Hauteur du Ventoux » : « Ventoux, 91940 Les Ulis se situe à environ 48.677752° N et 2.177337° E. »
- « Hauteur du Mont Ventoux » : Mont Ventoux, 84340 Beaumont-du-Ventoux se situe à environ 44.173964° N et 5.278287° E.

Pour ces deux derniers cas, le LLM ne semble pas appeler le service ALTITUDE et renvoie simplement les coordonnées (service GEOCODE).

Ces quelques exemples illustrent l'importance du LLM dans le traitement. Il doit être en capacité de :

- Extraire le toponyme de la question initiale,
- Choisir le toponyme dans une liste,
- Identifier la ou les actions à réaliser ainsi que leur ordre.

Un équilibre sensible entre probabilité et déterminisme

Si la mise en œuvre technique des composants et leur connexion ne présente pas de grandes difficultés techniques (avec une documentation *ad hoc* et dans un contexte de test pour cet article), le point sensible de cette interface repose sur « l'ajustement » du dialogue du LLM et du client MCP. Or ces deux composants évoluent dans deux logiques différentes :

- Le LLM est basé sur une approche probabiliste : il interprète le texte soumis ou génère du texte.
- Le client MCP produit des textes formatés (déterminés) devant être exécutés par le serveur MCP. Cela laisse assez peu de place à la créativité souvent riche d'un LLM !

Les principaux points de vigilance sont :

- Le niveau de compréhension et d'interprétation de la requête par le LLM,
- Le choix des outils à mobiliser pour réaliser la tâche (par exemple, le MCP de QGIS propose plus de 110 fonctions),
- L'orchestration des outils.

Face à ces limitations, il est possible d'aider le LLM en contraignant ou en orientant certaines étapes de son interprétation, par exemple :

- Sur le choix des fonctions en procédant à des classement fonctionnels pré définies des outils,
- Sur l'ordre de réalisation des tâches.

Ces informations peuvent être portées par le client MCP lors des échanges avec le LLM afin d'orienter sa prise de décision, puis être prises en compte lors de la construction des appels vers le serveur MCP.

Mais, si cette part de déterminisme permet de limiter le champ des possibles dans l'interprétation du LLM, elle introduit le risque de ne pas couvrir tous les champs fonctionnels ou processus susceptibles d'être rencontrés !

Tout l'enjeu est donc de **trouver un équilibre entre la capacité de création du LLM et le formalisme requis pour solliciter les services MCP.**

Conclusion

Encore récente, l'interaction en langage naturel avec les outils SIG ouvre des perspectives intéressantes de démocratisation dans l'accès aux outils et dans développement des usages.

Cependant, la réalisation de ce type d'interface se singularise par la nature même du LLM, qui est en capacité de générer et interpréter du texte. La difficulté est de maîtriser cette « créativité » pour la contraindre dans le formalisme attendu par le service applicatif MCP. L'interface MCP se différencie donc nettement des interfaces courantes entre machines (via API) dans lesquelles les messages échangés sont formatés a priori. Et au-delà de cette particularité, cette interface MCP a également des impacts importants car :

- elle induit une complexification de l'architecture technique,
- elle renforce des dépendances à des outils ou services tiers parfois commerciaux (LLM) pouvant induire des coûts (token) pas toujours anticipables.

La mise en place de tels outils doit donc être évaluée avec soin en fonction de la réelle plus-value observée chez les utilisateurs compte tenu des impacts techniques, fonctionnels et financiers sans oublier la finesse du paramétrage du MCP. Une véritable montée en compétence sur l'outil ne doit pas être écartée. Mais cela est un autre débat...

Exemple de description de fonctions exposées par la MCP.

MCP de l'IGN (<https://geollm.beta.ign.fr/geocontext/mcp>)

Outil : geocode

Description : Renvoie des résultats d'autocomplétion géocodés à partir d'un texte libre (lieu, adresse, POI), avec coordonnées, libellé complet et informations de localisation (`kind`, `city`, `zipcode`). Les coordonnées `lon/lat` retournées sont directement réutilisables dans tous les autres tools. Le champ `kind` indique le type de résultat (ex : `monument`, `street`, `city`, `locality`). (source : Géoplateforme (service d'autocomplétion)).

Schéma :

```
{
  "type": "object",
  "properties": {
    "text": {
      "type": "string",
      "description": "Le texte devant être complété et géocodé",
      "minLength": 1
    },
    "maximumResponses": {
      "type": "integer",
      "description": "Le nombre maximum de résultats à retourner (entre 1 et 10). Défaut : 3.",
      "minimum": 1,
      "maximum": 10
    }
  },
  "required": [
    "text"
  ]
}
```

Liens :

- <https://www.arcorama.fr/2026/07/arrivee-de-mcp-dans-arcgis-pourquoi.html>
- https://plugins.qgis.org/plugins/qgis_mcp_plugin/