

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Chemical Process Safety Analysis MCP

Turn HAZOP data into actionable risk mitigation plans.

Chemical Process Safety Analysis MCP gives your AI client the specialized logic needed for petrochemical risk management. It handles everything from identifying hazardous event sequences to calculating necessary Safety Integrity Levels. Instead of manually parsing HAZOP deviations, you can use your agent to model physical impacts and evaluate the overall safety health of a unit in seconds.

hazop

sil

safety

chemical

risk



The connectivity layer between AI and the world's software.



Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest
managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.

— Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT`https://edge.vinkius.com/{token}/mcp`

Claude



Cursor



VS Code



Windsurf



Grok



Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1)
Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

Get started at cloud.vinkius.com — connect your AI agent in under 60 seconds.

Chemical Process Safety Analysis MCP

4 tools available

Cloud-hosted on Vinkius

You can now bring specialized petrochemical safety logic directly into your AI workflow. This MCP bridges the gap between raw HAZOP studies and the technical data required for real risk assessment. When you work with complex petrochemical units, you need more than just text analysis; you need mathematical modeling and standardized safety calculations.

Your agent uses this MCP to identify specific hazardous event sequences based on deviations you provide. Once a scenario is identified, the tool calculates the physical impact of that event. It also handles the heavy lifting of determining the required Safety Integrity Level (SIL) to mitigate identified risks. Rather than jumping between spreadsheets and modeling software, you can stay within your coding or chat environment to get high-level safety health summaries for your entire process unit. It turns your AI client into a specialized safety engineering partner.

Core Capabilities

01 — Hazard Identification

Your agent uses HAZOP deviations to map out potential dangerous event sequences.

02 — Impact Modeling

The AI calculates the physical consequences and impact radii of specific hazards.

03 — SIL Determination

The tool calculates the required Safety Integrity Level based on your specific risk tolerance.

04 — Safety Health Auditing

Your agent can generate high-level summaries of the safety status for entire petrochemical units.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/chemical-process-safety-analysis — connect your AI agent in three steps.

- 01 Connect your preferred client like Claude or Cursor to Vinkius.
- 02 Provide HAZOP deviations or scenario data to your AI agent.
- 03 The agent calls the specific MCP tool to run calculations or models.
- 04 Receive technical results like SIL ratings or impact radii directly in your chat.

You connect the MCP to your AI client and start feeding it process data.

Built For

This MCP is built for engineers working in high-stakes petrochemical and chemical processing environments.

Process Safety Engineer

Uses the MCP to automate the translation of HAZOP findings into risk models.

Risk Assessment Specialist

Hands off raw deviation data to the AI to get rapid SIL and consequence calculations.

Plant Manager

Uses the safety health summary tool to get a quick pulse on unit integrity.

What Changes When You Connect

- 01 Converts HAZOP deviations into structured hazard sequences.
- 02 Calculates specific SIL requirements based on risk tolerance.
- 03 Models physical impacts like toxic release radii.

04 Provides rapid safety health summaries for entire units.

Real-World Applications

HAZOP Follow-up

After a HAZOP study, use the MCP to immediately model the consequences of the identified deviations.

Risk Mitigation Planning

Determine the exact SIL rating needed for a specific safety instrumented function.

Emergency Response Prep

Model the impact radius of a toxic release to plan evacuation or containment zones.

Safety Auditing

Get a high-level overview of a unit's safety status to prepare for regulatory reviews.

Patterns to Avoid

Vague hazard descriptions

❌ AVOID

You tell your agent to look for any possible danger in a refinery unit without providing specific data.

✓ INSTEAD

Provide specific HAZOP deviations to your agent so it can use `analyze_hazard_scenarios` to map out actual event sequences.

Ignoring physical impact

❌ AVOID

You identify a leak but skip the step of figuring out how far the toxic cloud actually travels.

✓ INSTEAD

Use `model_consequences` to calculate the specific impact radii and physical effects of the hazard you identified.

Manual SIL guesswork

❌ AVOID

You pick a Safety Integrity Level based on gut feeling instead of calculated risk tolerance.

✓ INSTEAD

Run `calculate_sil_requirements` to get the exact mitigation level needed for your specific safety limits.

The Right Fit

Process safety engineers and risk specialists should connect this MCP to automate the math behind HAZOP studies. Plant managers who need quick unit health checks will find it useful. If your team relies solely on manual spreadsheet entry and doesn't use structured deviation data, this MCP won't provide the technical depth you need.

4 Specialized Tools for Chemical Process Safety Analysis

These tools turn raw HAZOP deviations into actionable risk models and safety integrity calculations.

#	TOOL	DESCRIPTION
01	evaluate_process_safety_status	This tool provides a high-level summary of a petrochemical unit's safety health. It gives you a quick overview of the current safety standing of a process.
02	analyze_hazard_scenarios	This tool identifies and categorizes potential hazardous event sequences. It uses HAZOP deviations to map out how a process failure might unfold.
03	model_consequences	This tool estimates the physical impact of a specific hazard scenario. It calculates how a hazard actually affects the surrounding environment or equipment.
04	calculate_sil_requirements	This tool determines the necessary Safety Integrity Level (SIL) for a risk. It calculates the specific mitigation level required to keep a process within safety limits.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Identify hazard scenarios for these HAZOP results: [{'deviation': 'High Pressure', 'cause': 'Valve Failure', 'consequence': 'Overpressure'}] with conditions {'temp': 350, 'pressure': 20}.



The identified scenario is a high-pressure event caused by valve failure, classified as an explosion hazard.

U What is the impact of scenario SCEN-123 involving a toxic release of Ammonia?



The toxic release of Ammonia for scenario SCEN-123 results in an impact radius of 450 meters with a peak concentration exceeding safety limits at the source.

U What SIL is required for scenario SCEN-456 if my risk tolerance is low?



For scenario SCEN-456 with low risk tolerance, a SIL 3 rating is required to ensure sufficient mitigation.

Frequently Asked Questions

01 What kind of data does this MCP need?

It works best with HAZOP deviations, process conditions like temperature and pressure, and specific hazard scenarios.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 Does it calculate SIL levels?

Yes, the `calculate_sil_requirements` tool determines the necessary Safety Integrity Level based on the risk and your tolerance.

04 What is the main use for the consequence modeling tool?

The `model_consequences` tool is used to estimate the physical impact, such as the radius of a toxic release, for a specific hazard.

05 Is this for general safety or petrochemicals?

This MCP is specifically designed for petrochemical process safety management and HAZOP-based workflows.

06 How do I identify potential hazards from my HAZOP study?

You can use the `'analyze_hazard_scenarios'` tool by providing your HAZOP deviations and current process conditions as JSON strings.

07 Can I determine the required Safety Integrity Level (SIL)?

Yes, the `'calculate_sil_requirements'` tool calculates the necessary SIL based on a specific scenario ID and your chosen risk tolerance level.

08 How is the physical impact of a chemical release estimated?

The `'model_consequences'` tool estimates the impact radius and peak impact values for a specific scenario using provided chemical properties.

Go Live in 60 Seconds

Get your connection token from cloud.vinkius.com, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

`https://edge.vinkius.com/[TOKEN]/mcp`

CLIENT	WHERE TO CONFIGURE
 Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
 Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
 VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add <code>"chemical-process-safety-analysis": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → Add endpoint URL
 ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
 Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

-  **Ask ChatGPT** 
-  **Ask Claude** 
-  **Ask Perplexity** 
-  **Ask Gemini** 
-  **Ask Grok** 

READY TO CONNECT

Chemical Process Safety Analysis is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and
start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Chemical Process Safety Analysis. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	Chemical Process Safety Analysis MCP
Server ID	01a096a9-ff6e-7220-ae3e-028f54d74c15
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/en/ai-agent-connect/chemical-process-safety-analysis.