  
  
  
  
  
  
  
  
  
  
  
  
  
**Version: v1.0  
Name: Qimin Zhao**This invention is currently under active examination by both the China National Intellectual Property Administration (CNIPA) and the United States Patent and Trademark Office (USPTO), and is fully protected under international patent law.  
**License Policy**  
The Semantic Chain Security Model (SCSM), including its patented semantic behavior chain modeling methods, architectural constructs, pivot point semantics, behavior coordinate definitions, and AI-driven reasoning processes, is **strictly licensed under the following two models only**. **No other licensing pathways are available.**   
1.Enterprise Annual License Model: For commercial enterprises, licensing is offered on an annual fee basis, with an initial term of at least one (1) year and a maximum term of three (3) years. For enterprises demonstrating strategic long-term integration needs, license terms exceeding five (5) years may be negotiated on a case-by-case basis. A maximum of three (3) enterprise licenses may be executed per calendar year to maintain ecosystem strategic control. Licenses are strictly limited to internal use and prohibit sublicensing, resale, or use in derivative commercial products intended for third-party distribution.   
2.Government / Defense / Energy and Critical Infrastructure One-Time Internal Use License: For government entities, military and defense organizations, energy sector operators, and other national critical infrastructure operators, licensing is provided as a one-time internal-use license. Such licenses are strictly limited to internal deployment within the licensee’s own systems and environments. Any form of sublicensing, resale, embedding into externally distributed products or services, or derivative commercialization is strictly prohibited. The Licensor reserves the right to audit compliance with the license scope. The Licensor retains full ownership and management rights of all intellectual property covered by the SCSM patent family. Any unauthorized use, sublicensing, derivative commercialization, or transfer constitutes infringement and will be subject to legal enforcement.  
  
 **The following terms govern all usage, reference, standardization, and implementation of this method:**

1. Source Protection and Commercial Restriction

Due to the structural flexibility and universal applicability of this method, it is officially classified as **closed-source**.

No government body, energy sector entity, institutional body, or commercial organization may use, replicate, adapt, or integrate this method in any form without prior written authorization from the patent holder.

**Unauthorized deployment—whether embedded into a product, used for internal processes, or applied for investigative purposes—constitutes a violation of intellectual property rights.**

2. Terminology Use by Standards Bodies

To promote industry-wide semantic alignment, standardization organizations are permitted to reference or formalize terminology derived from this method, provided the following conditions are met:

Use is restricted to documented terminology only (e.g., "Behavior Chain", "Pivot Strength", "Semantic Reasoning Layer", etc.)

No implementation paths, logical flow structures, or reconstruction logic may be replicated without patent holder authorization

Any use must be aligned with the unified consent of the patent inventor(s)

3. Academic and Research Use (Free Authorization)

Universities and research institutions may be granted free access, subject to the following categories:

3.1. For Academic Publications (No Authorization Required)

Use of terminology or theory in academic papers, presentations, or public research that does not involve implementation, experimentation, or system deployment is freely allowed without prior authorization.

3.2. For Experimental Implementation (Authorization Required)

Any attempt to build, simulate, or test the method—even for non-commercial purposes—must be registered under the AI Security Investigation Alliance (AISIA) and linked to a formal research project.

Prior written authorization is required before any such implementation.

4. Unauthorized Internal Deployment Constitutes Infringement

Any government agency, energy provider, institutional user, or commercial organization that internally builds, integrates, or deploys this method—even without direct product integration—will be considered to have infringed the patent.

5.Attempts to bypass protection through terminology substitution, minor logic alterations, or derivative reconstructions are equally considered infringements.

6.Any licensed integration must preserve the author-defined semantic layers and the integrity of the behavior chain. All referenced terminology, structures, or conceptual frameworks must explicitly acknowledge the original source and inventor attribution.

This includes any use for:

**Internal security event investigation**

**System behavior reconstruction**

**Analytical workflow based on this method's logic**

No distinction is made between deployment methods (script, API, workflow engine, etc.). Any unlicensed use is considered infringement, regardless of scale or intent.

Enforcement Clause

The patent holder reserves the right to pursue legal action and compensation for any unauthorized use, reproduction, or implementation. Licensing inquiries may be directed to the inventor via formal request channels.