

Yury Sidarenka

Principal Enterprise Architect | Cloud, AI & Platform Architecture
Highlands Ranch, CO 80126 • 720-236-0601 • yury.sidarenka@gmail.com
linkedin.com/in/yurysidarenka • yury.sidarenka.com

PROFESSIONAL SUMMARY

Principal Enterprise Architect with 20+ years of experience designing and modernizing large-scale distributed systems, including nearly a decade in highly regulated financial services and lending.

Combines enterprise architecture leadership with deep hands-on engineering across cloud platforms, distributed systems, API and integration architecture, zero-trust security and identity across employees, partners, and customers (Entra B2B/B2C, PIM/PAM with CyberArk, passwordless), platform engineering, and enterprise delivery automation.

Turns architecture into measurable business outcomes by leading through influence and helping teams make the right architecture decisions on their own: a zero-trust Istio service mesh replacing end-of-life ingress across all production workloads with no business disruption; an Architecture Review Board, architecture standards, and playbooks built from scratch and adopted enterprise-wide; and about a 90% reduction in cloud log-ingestion costs through telemetry standards and cost awareness.

Advances applied and agentic AI across software engineering and enterprise knowledge workflows, including RAG, MCP, multimodal systems, multi-agent orchestration, and an agentic SDLC on GitHub Agentic Workflows with human approval gates, with governance grounded in security, compliance, and regulatory requirements.

CORE COMPETENCIES

Enterprise & Solution Architecture • Technology Strategy & Modernization • Distributed Systems • Applied AI & Agentic Systems • Enterprise AI Platforms & AI-Assisted Engineering • Agentic SDLC • Azure & AWS Cloud Architecture • Data & Analytics Architecture • Zero-Trust Security, Identity & Privileged Access (B2B, B2C) • Kubernetes & Cloud-Native Platforms • Platform Engineering & Delivery Automation • Event-Driven & Microservices Design • Observability & SLOs • Legacy Modernization • Architecture Governance (ARB, ADRs, Standards) • Technical Leadership & Mentorship

PROFESSIONAL EXPERIENCE

Principal Enterprise Architect

August 2024 – Present

Pulte Mortgage | Denver, CO

- Provide enterprise architecture direction across the IT portfolio, 30+ concurrent projects and initiatives from early outlines and intake through delivery, supporting 8+ delivery teams and aligning Application Development, Infrastructure, DevOps, and Security around a common cloud modernization strategy.
- Established and chair the **Architecture Review Board (ARB)**: researched governance practices across organizations, defined the submission, review, and decision-recording process, and published it company-wide; architecture decisions now flow through the ARB with ADRs and documented trade-offs.
- Self-initiated the **Enterprise Standards Domain**, a single home for architecture standards built on **RFC 2119 requirement levels** (MUST / SHOULD / MAY mapped to critical / major / minor) with a defined contribution model; adopted enterprise-wide, starting with Infrastructure and DevOps.
- Lead architect for five strategic initiatives, including four mortgage-technology vendor integrations and a document-management cloud migration. Initiated each, designed the solution architecture, established the infrastructure, CI/CD, security, and integration foundations, and guide engineering teams through delivery.
- Led the migration from end-of-life NGINX ingress to **Istio Gateway API** with sidecarless ambient mesh, cutting over all production workloads with no business disruption and making **AKS** zero-trust by default with mTLS. Introduced **Calico** network segmentation, automated certificate management with cert-manager and Key Vault, Helm deployment standards, **KEDA** event-driven autoscaling, and blue/green and dark-launch release patterns.
- Designed the enterprise **Zero-Trust API and workload identity** architecture, standardizing Entra ID, OAuth 2.0/OIDC, AKS Workload Identity, user-assigned managed identities, centralized authorization, and private networking, and extended it to legacy on-premises IIS APIs through Azure Arc.
- Architected **customer and partner identity (CIAM)** for internal and external users: Entra ID for employees, **Entra B2B** for partners, vendors, and guest users, and **Azure AD B2C / Entra External ID** for external customers, with SSO, MFA, Conditional Access, and **passwordless authentication** with Microsoft Authenticator. Replaced stored secrets with **federated credentials** (workload identity federation) for GitHub Actions pipelines, AKS workloads, and service-to-service access.

- Partnered with the Security team to set up and operate **privileged access management: CyberArk** for vaulted privileged credentials and controlled access to servers, and **Entra PIM** for just-in-time administrative roles.
- Built a shared CI/CD orchestrator on GitHub Actions, taken from concept to production: versioned, reusable workflows with standard build, security-scanning, and deployment gates, OIDC and managed identity authentication, and a hybrid GitHub-hosted and private self-hosted runner model.
- Designed enterprise **event-driven and distributed processing patterns** using Azure Service Bus sessions for per-loan ordering and concurrency control, idempotent command processing, blob-backed large payloads, status APIs, dead-letter handling, retries, correlation, and downstream domain events.
- Reduced **PCI DSS compliance scope** by redesigning payment architecture around Stripe-managed payment data, retaining only protected payment references internally and introducing network, identity, and AKS isolation controls; produced supporting architecture, network, and audit documentation.
- Traced a major Log Analytics cost leak to its root causes and eliminated it, producing substantial recurring cloud savings. Established enterprise **observability standards** using OpenTelemetry, Azure Monitor, and Application Insights, including distributed tracing, structured logging, correlation IDs, SLO-driven dashboards, alerting standards, telemetry filtering, and ingestion-cost controls.
- Drive enterprise adoption of applied and **agentic AI**, including RAG, MCP, multimodal AI, model routing, and multi-agent orchestration, on a governed Azure AI platform built on Microsoft Foundry with parameterized IaC controlling models, capacity, networking, and access per environment. Designed the Loan Intelligence Workspace, a per-loan semantic knowledge layer combining loan data, documents, pricing, conditions, and events with evidence-grounded AI retrieval.
- Launched a shared Agent Plugins Marketplace for GitHub Copilot and Cursor, built an AI pull-request reviewer that cites the exact standard behind each finding and ranks it by severity, and proved a repeatable pattern for exposing enterprise APIs to AI agents through MCP, secured with Entra ID and API Management.
- Built a **GitHub Agentic SDLC on GitHub Agentic Workflows (gh-aw)** and Copilot agents that turns an Azure DevOps or Jira user story into a plan, code, tests, and a pull request, using an orchestrator with specialist sub-agents, an independent PR-review agent, human approval gates, and OIDC federated credentials with no stored secrets.
- Built an AI-agent document splitting and classification solution to replace retired ABBYY FlexiCapture; tested on production-volume documents and modeled at roughly 10% of the legacy cost, restoring automation to a process that had become manual.

Technologies: Azure · C# / .NET · Microsoft Foundry · Azure OpenAI · Azure AI Search · Document Intelligence · Microsoft Fabric · MCP · RAG · Multi-Agent Systems · GitHub Copilot · GitHub Agentic Workflows (gh-aw) · Copilot Agents · Cursor · AKS · Kubernetes · Istio Ambient · Gateway API · cert-manager · Calico · Docker · Helm · Bicep · GitHub Actions (reusable workflows) · Azure DevOps (Boards, Wiki) · KEDA · Entra ID · Entra B2B · Azure AD B2C / Entra External ID · Conditional Access · SSO / MFA · Passwordless · Microsoft Authenticator · CyberArk (PAM) · Entra PIM · Federated Credentials · Workload Identity · Managed Identity · Azure Arc · Key Vault · Application Gateway · API Management · Azure Service Bus · Azure Blob Storage · Event Grid · App Configuration · Azure SQL · Cosmos DB · OpenTelemetry · Application Insights · Azure Monitor · Log Analytics · OAuth 2.0 / OIDC · RBAC · Private Endpoints · Stripe · PCI DSS · Zero Trust

Software Architect / Solution Architect

May 2017 – August 2024

Nelnet Inc. | Centennial, CO

- Led architecture for the modernization of a large-scale financial services platform serving **40+ million customers**, evolving monolithic applications toward distributed microservices while strengthening security, scalability, resilience, and performance.
- Architected and led the migration of **25+ enterprise applications from on-premises infrastructure to AWS**, defining cloud architecture patterns across compute, networking, identity, security, integration, and serverless services.
- Modernized legacy data access across **IBM i and SQL Server**, introducing API-based integration and Redis-backed caching patterns that decoupled consuming applications from underlying systems and improved performance and reuse.
- Defined and communicated enterprise **technology strategy, architecture standards, and modernization patterns**, using architecture fitness functions to continuously evaluate alignment with target-state principles.
- Designed reusable **enterprise APIs, integration services, and shared architecture capabilities** supporting multiple products and business units, reducing duplicated implementations and enabling more consistent engineering patterns.
- Designed customer and employee identity: **Duende IdentityServer** as the identity provider for borrower-facing portals over OIDC/OAuth 2.0/JWT with MFA, and **Ping Identity** federated with **Azure AD / Entra ID** for internal-user SSO across company applications and enterprise APIs.
- Partnered with engineering leaders, system owners, program managers, and directors to turn business objectives into executable architecture, technical roadmaps, and cross-team modernization initiatives.

- Provided hands-on technical leadership and mentorship to engineering teams across distributed systems, cloud architecture, application security, API design, and modern software engineering practices.

Technologies: .NET / C# · RESTful APIs · OIDC / OAuth 2.0 / JWT · Duende IdentityServer · Ping Identity · Azure AD / Entra ID · SSO / MFA · Microservices · Service Discovery · Service Mesh · Docker / Containers · Terraform · AWS · Serverless Architecture · Kong API Gateway · WAF · HashiCorp Vault · Consul · Istio · Redis · SQL Server · IBM i · Entity Framework · NSwag · MediatR · TypeScript · JavaScript · Node.js · Angular · HTML5 · CSS / Sass / Less · NPM · Webpack · GitLab

Senior Software Engineer

January 2015 – April 2017

Location3 Media | Denver, CO

- Designed and built **LocalACT**, a suite of digital marketing tools supporting business listings, paid media, social channels, sales auditing, and administrative operations at scale.
- Developed full-stack applications using **C# / .NET, REST APIs, Angular/AngularJS, and TypeScript**, with SQL Server and Dapper providing the application data layer.
- Implemented cloud-based background processing and integration services with **Azure WebJobs, Azure Functions, and Azure Service Bus**, enabling asynchronous workflows and scalable application processing.

Technologies: C# / .NET · REST APIs · Angular · AngularJS · TypeScript · JavaScript · HTML5 · CSS · SQL Server · Dapper · Autofac · Azure WebJobs · Azure Functions · Azure Service Bus · NPM · Gulp · Webpack

Senior Software Engineer

November 2013 – December 2014

IHS Inc. | Englewood, CO

- Designed and developed **single-page web applications, REST APIs, and hybrid mobile solutions** that provided customers with real-time access to operational data and streamlined existing business workflows.
- Built an interactive **diagram authoring platform using JointJS** and developed cross-platform mobile applications with **Cordova/PhoneGap, KnockoutJS, and SignalR**, enabling responsive, real-time user experiences across desktop and mobile environments.
- Contributed across the full software development lifecycle, including application architecture, front-end and API development, integration, testing, and production support.

Technologies: C# / .NET · REST APIs · JavaScript · KnockoutJS · JointJS · SignalR · Cordova / PhoneGap · HTML · CSS

Software Engineer II

November 2010 – November 2013

EchoStar Corporation | Englewood, CO

- Designed and developed **web and desktop applications for set-top-box manufacturing and automated hardware testing**, improving test automation, deployment efficiency, and manufacturing quality.
- Helped reduce **test system costs by approximately 80%** by replacing and consolidating legacy testing capabilities with internally developed software solutions.
- Implemented **DirectShow-based video capture and hardware integration** across webcams and capture cards, with application data and test results stored across **MySQL, MongoDB, and RavenDB**.

Technologies: .NET / C# · DirectShow · Web Applications · Desktop Applications · MySQL · MongoDB · RavenDB · Hardware Integration · Automated Testing

EARLY CAREER

- **Software Engineer, BelStiepf** — Minsk, Belarus (August 2007 – November 2009). Built a trading and waybill application in C#/VB.NET on MS SQL Server deployed across 20+ stores, reducing required staffing by 20%; performed SQL Server administration and module design.
- **Software Engineer, Agat-System** — Minsk, Belarus (February 2005 – July 2007). Developed **APCO P25 digital radio communication software** in C/C++ for TI TMS320C55x digital signal processors (DSPs), including error-resistant coding, data exchange algorithms, and USB-based PC-to-radio communication; contributed to applications supporting a national radio network deployment.
- **Software Developer Assistant, Belarusian State University of Informatics and Radioelectronics** — Minsk, Belarus (September 2004 – January 2005). Developed a **C/C++ and Win32 API IQ-testing application** used in educational research.

TECHNICAL SKILLS

AI & Agentic Systems: Azure OpenAI · Anthropic Claude · Microsoft Foundry · Azure AI Search · Azure AI Services · Document Intelligence · AI Gateway (Azure API Management, LiteLLM) · RAG · Model Context Protocol (MCP) · Agent2Agent (A2A) Protocol · Multi-Agent Orchestration · Model Routing · Agentic Workflow Automation (n8n) · Tool / Function Calling ·

Planning · Structured Outputs · Multimodal AI · Intelligent Document Processing · Vector Search / pgvector · AI Evaluation · AI Governance & Guardrails

AI-Assisted Engineering: GitHub Copilot · GitHub Agentic Workflows (gh-aw) · Copilot Coding & Custom Agents · Claude Code · Cursor · Google Antigravity · VS Code · Agent Skills & Plugins Marketplace · AI Pull-Request Review · Agentic SDLC · Human-in-the-Loop Approval Gates

Cloud & Infrastructure: Azure · AWS · AKS · Application Gateway · API Management · Azure Front Door · Azure Service Bus · Event Grid · Azure Blob Storage · Key Vault · Entra ID · Managed Identity · App Configuration · Azure Functions · Azure Monitor · Azure Arc · Azure Container Registry · Azure Landing Zones · Hub-and-Spoke Networking · Private Endpoints · Private DNS · Serverless Architecture

Platform & DevOps: Kubernetes · Docker · Istio / Ambient Mesh · NGINX · Helm · GitHub Actions · Reusable Workflows · Azure DevOps · GitLab · Octopus Deploy · KEDA · Calico · Secrets Store CSI Driver · Actions Runner Controller · Bicep · Infrastructure as Code · Platform Engineering

Security & Identity: Zero Trust · OAuth 2.0 · OIDC · JWT · Entra ID · Entra B2B · Azure AD B2C / Entra External ID · CIAM · Passwordless Authentication · Microsoft Authenticator · CyberArk (PAM) · Entra PIM · Federated Credentials / Workload Identity Federation · GitHub OIDC · AKS Workload Identity · Managed Identity · Client Assertion / Certificate Authentication · Conditional Access · SSO · MFA / TOTP · HashiCorp Vault · Consul · Kong · Ping Identity · Duende IdentityServer · WAF · F5 · TLS / mTLS · RBAC · PCI DSS · NIST · OWASP · Section 508

Data & Analytics: Microsoft Fabric · Fabric Mirroring · Microsoft SQL Server · Azure SQL · Cosmos DB · PostgreSQL · pgvector · MySQL · Redis · MongoDB · RavenDB · IBM i · Entity Framework · Dapper

Observability & Quality: OpenTelemetry · Application Insights · Azure Monitor · Log Analytics · Distributed Tracing · Structured Logging · SLOs · Splunk · AppDynamics · SonarQube · k6 · Cypress · Selenium

Application & Integration: REST · OpenAPI / Swagger / NSwag · Event-Driven Architecture · Azure Service Bus · NServiceBus · MSMQ · CQRS · Idempotent Processing · JSON-RPC · MediatR · SignalR · Angular · React · Node.js · WPF · WCF · Kestrel · IIS · PWA · Capacitor / Cordova · Razor

Languages & Frameworks: C# / .NET · TypeScript / JavaScript · SQL / T-SQL · C / C++ · HTML · CSS / Sass / Less · LINQ · VB.NET · LabVIEW

Architecture Practice: Enterprise & Solution Architecture · Architecture Review Board (ARB) · ADRs · Reference Architectures · Architecture Standards · API-First Architecture · Distributed Systems · Microservices · Event-Driven Architecture · Domain Modeling · Integration Architecture · Platform Engineering · C4 / UML · Architecture Fitness Functions · Team Topologies · Blue/Green & Dark-Launch Delivery · Cloud Cost Optimization

Tools: Visual Studio · VS Code · Cursor · Claude Code · Antigravity · Jira · Confluence · GitHub · Bitbucket · Azure DevOps · GitLab

EDUCATION

Bachelor's and Master's Degrees in Telecommunication Networks and Devices

September 2000 – June 2005

Belarusian State University of Informatics and Radioelectronics | Minsk, Belarus

CERTIFICATIONS & PROFESSIONAL TRAINING

- [Microsoft Certified: Azure Solutions Architect Expert \(AZ-305\)](#) | Microsoft | November 2025
- [AWS Certified Solutions Architect – Associate \(SAA-C03\)](#) | AWS | March 2024
- [Kong Gateway Operations \(KGAC-201\)](#) | Kong | July 2022
- [Agentic AI Systems series \(8 credentials\)](#): Foundations of Agentic AI in GitHub · Agent Architecture and SDLC Integration · Multi-Agent Systems and Orchestration · Tooling, MCP, and Agent Execution Environments · Memory, State, and Evaluation · Governance, Guardrails, and Operations · Developing in Agentic AI Systems (Parts 1–2) | Microsoft Learn | October 2026
- [Creating a High Performance Culture](#) | LinkedIn Learning | April 2026
- [AI Agents for Production](#) | O'Reilly | January 2026
- [K8sGPT AI Learning](#) | O'Reilly | January 2026
- [Model Context Protocol \(MCP\): Hands-On with Agentic AI](#) | LinkedIn Learning | August 2025
- [AI on Azure: Intelligent Apps](#) | O'Reilly | July 2025
- [Certified LabVIEW Developer \(CLD\), 2012, and Associate Developer \(CLAD\), 2011](#) | National Instruments
- Earlier training: Project Management Introduction, DP Consulting Training Center (2008) · C/C++ Programming, BELHARD Training Center (2006)