Perry's Résumé - IT/OT Solution Architecture

Perry Kundert <*perry@kundert.ca*> `+1-780-970-8148`

2026-08-12 09:00:00

R&D engineer with 30+ years designing systems on both sides of the IT/OT boundary: SCADA protocol and RTU firmware controlling continent-wide pipeline infrastructure, and the integration, telemetry and service layers that carry operational data into enterprise systems. Author of `cpppo`, the Python EtherNet/IP and CIP library used globally as the integration layer between analytics and the plant floor, and of the `datasim` large-scale PLC simulation environment used to de-risk a production SCADA transition. Most recent, built secure unidirectional DNP3 field-data paths and deployment/test automation for Ignition.

Architecture practice built on the assumption that components fail, links degrade, and adversaries are competent: systems designed to continue operating through partial failure. (PDF, Text)

TECHNICAL SKILLS

Solution Architecture	IT/OT integration design, cross-system impact and dependency analysis, build-vs-buy and vendor-reversibility assessment, reusable integration patterns, technology roadmapping
Integration & Enterprise Platforms	SOA and RESTful APIs, multi-tier client/server, distributed authentication and session management, message and telemetry pipelines, historian and analytics data paths, CAP/BFT design
OT/ICS	Ignition SCADA (deployment automation, scripting regression), PLCs, HMIs, RTU firmware, OT network segmentation, data diodes and unidirectional gateways, large-scale PLC/RTU simulation
Industrial Protocols	DNP3, EtherNet/IP, CIP, Modbus/TCP, proprietary SCADA protocols, Reed-Solomon FEC, multi-route fault-tolerant comms
Networking & Transport	TCP/IP, DNS, HTTP/HTTPS, QUIC, mTLS 1.3, WebSockets, WebTransport, satellite and degraded-link WAN engineering
Security & Cryptography	PKI, Ed25519, WebAuthn/FIDO2 and passkey architectures, cryptographic protocols, secret sharing, zero-trust access, PQC
AI/ML Deployment	Production LLM services, multi-backend portability, KV prompt caching, retrieval over controlled corpora, on-premises inference for data-sovereignty-constrained workloads
Languages	C++ (25+ yrs), Python (15+ yrs), Rust (5+ yrs), C, Go, SIMD
Delivery & Infra	Linux, Docker, CI/CD, Nix reproducible builds, Cloudflare Zero Trust, code review and mentorship, Scrum/Agile delivery

ARCHITECTURAL PERSPECTIVE

IT and OT security are in rapid transition, and the transition is structural rather than incremental.

- Conventional defences are O(1): a firewall, a directory, a credential store. Compromise the single gatekeeper and the entire estate follows. The defences displacing them are O(N): passkeys and hardware-bound credentials held independently by each of N participants, each requiring separate attack, with no repository whose capture yields the whole.
- The same asymmetry now runs the other way on knowledge. An AI-enabled attacker can read, correlate and reason over a standardized defensive posture (the published frameworks, the known default configurations, the vendor documentation) faster and more completely than the defenders maintaining it. Standardization that once produced auditability now also produces a fully enumerable attack surface.
- The practical conclusion: perimeter-centric architecture is a Maginot Line. Designs must assume the boundary is already crossed and make the interior expensive: distributed credentials, per-actor authorization, protocols that degrade rather than fail open, and control paths that remain correct under partial compromise.

RELEVANT EXPERIENCE

IT/OT Solutions Engineer - *Vantage Engineering* (Spruce Grove, AB 2026–Present)

Designing and delivering the boundary itself: unidirectional field-data paths, SCADA deployment automation, and business tooling built on top of the resulting data.

- Developed a secure DNP3 data diode supplying real-time field data to IT systems while leaving the OT field equipment unreachable from the IT side. Dramatically reduced both up-front acquisition and ongoing operating cost against commercial diode products, without relaxing the unidirectional guarantee.
- Implemented dev, staging and production deployment infrastructure for Ignition SCADA, automating regression testing of Ignition Python scripting: a capability the vendor does not currently offer. Script changes are now validated before they reach production rather than in it.
- Developed `localwebauthn`, a self-hosted WebAuthn relying-party library: passkey authentication with no dependence on an external identity provider, and no credential repository whose capture would yield the estate. Suitable for OT-adjacent systems that must authenticate strongly while remaining operable when the wider network or the internet is not.
- Deliver prototypes of custom tooling to business users, giving them direct control of vendor WIP quotes, invoicing, timekeeping and expensing, while preserving the accountant's traditional controls over the ledger.

R&D Consultant & Solution Architect - *Dominion R&D Corp.* (Remote, 2009–Present)

Architecture and delivery of integration, telemetry and security systems spanning the IT/OT boundary for energy, utility and fintech clients.

- Created `cpppo`, the widely used Python EtherNet/IP and CIP protocol library: the inspectable integration layer between enterprise analytics and the PLCs on the plant floor, in place of a vendor black box.

- Built `datasim`, a Docker-based large-scale PLC simulation environment (dozens to hundreds of concurrent simulated PLCs, each with its own network stack) supporting Modbus, EtherNet/IP and a web API front end. Records and replays real field data, and injects controlled latency, packet loss, bandwidth limits and per-PLC transaction capacity, so a SCADA vendor's polling behaviour is measured against degraded WAN and satellite routes before cutover rather than after. Used to de-risk a production SCADA transition.
- Designed and implemented a complete EVM smart-contract system: ERC-20 with identity-aware transfers, ERC-721 insured-asset tokens, parametric insurance contracts, and a privacy-preserving bearer-note layer on Groth16 SNARKs over Poseidon Merkle commitment pools, verified end-to-end on BN254. Delivered concurrently with full-time client work through disciplined AI-accelerated R&D: LLM output treated strictly as hypothesis, with no model assertion admitted to a design until confirmed by execution or independent derivation.
- Developed `ezpwd-reed-solomon`, high-throughput C++/JS/Python Reed-Solomon and BCH codecs, used by aerospace and defence developers globally.
- Architected and deployed `BUCKy`, a production generative AI service: multiple interchangeable inference backends (hosted API, local Ollama, local MLX) with vendor reversibility as a first-order design constraint; a ~100K token knowledge base pre-computed once into a KV prompt cache and cloned per session copy-on-write; delivered publicly through a Cloudflare Zero Trust tunnel with no inbound exposure of the host.
- Delivered ruggedized satellite-connected monitoring, communications and video systems across Alberta oilfields; field-serviceable, and diagnosable from 400 km away.
- Guide client development teams through cryptographic, distributed-systems and industrial integration architecture; author technical articles on industrial communications, consensus, and monetary system design.

Software Engineer - *clearGRID Ltd.* (Kelowna, BC 2017–2022)

Replaced expensive proprietary radio telemetry with commodity SDR hardware: a build-vs-buy case argued on cost, then made to hold in the field.

- Built an end-to-end real-time receiver decoding 64 concurrent channels from a 25 Msps I/Q stream on commodity x86 and ARMv8, sustained, with no dropped samples.
- Designed the polyphase filterbank channelizer and window/DFT chain; hand-optimized hot paths in AVX and NEON.
- Reached agreement on meter readings across lossy RF channels without requiring global coordination.
- Built a recorded-signal regression harness so algorithm changes were measured against real captured field data rather than synthetic benchmarks.

Distributed Systems R&D - *Holo Ltd.* (Kelowna, BC 2018–2020)

Architected and tested prototypes of HoloFuel's novel transaction engine.

- Designed and validated atomic transaction processing under simulated network partitions.
- Implemented agent-centric accounting enabling linear O(n) scaling in place of $O(n^2)$ global consensus bottlenecks.
- Contributed R&D to Holochain's agent-centric distributed architecture.

Sr. IT Advisor - *Enbridge Pipelines* (Edmonton, AB 2002–2009)

Reduced the risk profile of a hydrocarbon pipeline control system with a cryptographically secure multi-route communications protocol.

- Architected the LiveWIRE fault-tolerant Reed-Solomon encoded multi-route protocol for real-time SCADA telemetry over marginal and intermittent links, maintaining cryptographic integrity across untrusted network segments.
- Developed solid-state RTU firmware for continuous 24/7 control; sustained <1 defect per 10K LOC as measured in the field, not in the lab.
- Deployed hundreds of ruggedized units across critical infrastructure sites.

Software Developer - *Hewlett-Packard* (Calgary, AB 1989–1996)

Pioneered a radical re-architecture of a core SCADA automation alarm system component.

- Re-engineered RTAP's core alarm engine with DFA state machines.
- Enabled end-users to configure complex, geographically distributed safety-critical workflows.
- Still deployed in pipeline SCADA systems continent-wide, 30+ years on.

OPEN SOURCE & PUBLICATIONS

- cpppo - Industrial EtherNet/IP, CIP and Modbus protocol implementation (Python)
- ezpwd-reed-solomon - High-performance Reed-Solomon and BCH FEC (C++/JS/Python)
- python-slip39 - SLIP-39 Shamir secret sharing for seed backup and recovery
- crypto-licensing - Ed25519-signed license verification with DNS-based key distribution
- Technical articles on industrial communications, consensus algorithms, distributed systems security, and monetary system architecture.

EDUCATION

B.Sc. Computer Science - *University of Calgary* (Calgary, AB 1984-1989)