THE GREEN DASHBOARD FALLACY

Unified Information Potential in Rare-Event Predictive Integrity Detection

DOCUMENT CONTROL	
DOC-ID:	FSME-WP-UIP-01
REVISION:	1.0 — Initial Release
DATE:	2026
STATUS:	CLEARED FOR PUBLIC RELEASE
IP STATUS:	Proprietary & Trade Secret Protected | FSME Logic
AUTHOR:	Alexander Kalyniuk | FSME Logic | Edmonton, Alberta, Canada

ABSTRACT

Standard industrial monitoring infrastructure is designed to detect the symptoms of mechanical failure. It is not designed to detect failure itself. By the time a monitored signal breaches a preset alarm threshold, the physical damage causing the breach has already occurred. This document presents the Unified Information Potential (UIP) framework — a physics-based approach to predictive integrity monitoring that measures the structural health of a signal rather than its amplitude. UIP detects kinematic signature degradation — the measurable loss of signal elasticity that precedes mechanical failure — weeks or months before any amplitude threshold would trigger. The framework has been benchmarked against publicly available datasets spanning industrial machinery, aerospace systems, orbital spacecraft telemetry, and quantum hardware. In every domain, the same physical signature of degradation was detected without domain-specific retraining, confirming that the underlying physics is universal. No training data, cloud infrastructure, or new sensor hardware is required.

> A degrading system loses its complex dynamic equilibrium before it loses its function. **FSME Logic measures that loss directly.**

FSME Logic | alex-kalyniuk@fsmelogic.ca | fsmelogic.ca | Edmonton, Alberta, Canada

EXECUTIVE SUMMARY

The Problem. Industrial monitoring systems generate confidence, not certainty. When every dashboard is green, operations personnel conclude that assets are healthy. This conclusion is structurally false. Threshold alarms measure amplitude — how large a vibration is, how high a temperature has climbed. They do not measure the underlying physical process producing those amplitudes. Sub-surface stress accumulation, bearing fatigue, hydraulic crystallization, and gearbox micro-fracture all produce measurable signatures in the information structure of a signal long before they produce amplitude changes. Standard monitoring is blind to these signatures. The dashboard is green. The asset is dying.

The Framework. The UIP framework treats signal health as a physical property. A healthy system maintains structural coherence state — baseline operational variance in its output signal reflecting the system's internal degrees of freedom. A degrading system loses this elasticity. The signal becomes constraineder, more predictable, more repetitive before it becomes louder or hotter. UIP quantifies this loss using a advanced time-series behavioral memory framework that accounts for the signal's memory — the way the present state of a signal carries information about its past. When that memory begins to break down in a characteristic pattern, UIP flags it as a pre-failure signature.

Cross-Domain Validation. The same engine, running identical parameters without domain-specific retraining, has produced consistent pre-failure detection across industrial bearings, hydraulic systems, turbofan engines, orbital spacecraft, Mars rover actuators, gravitational wave observatories, and quantum processor arrays. Cross-domain consistency is the defining characteristic of a physics-based framework. A statistical model trained on one domain fails in another. Physical law does not.

Practical Implication. FSME Logic delivers predictive lead time through forensic audit engagements. A client provides raw historical telemetry from an asset that experienced an unexpected failure. FSME Logic processes it on air-gapped hardware and returns a forensic report demonstrating whether UIP would have detected the pre-failure signature before the SCADA alarm triggered. No cloud. No new sensors. No training data. No integration. The audit fee is credited toward any subsequent fleet-wide engagement.

1.0 THE PROBLEM: THE GREEN DASHBOARD FALLACY

This document begins with a scenario familiar to any reliability engineer who has been responsible for a major asset failure.

> "A critical asset suffered a catastrophic mechanical failure. The vibration sensors, thermal monitors, and SCADA threshold alarms showed completely normal, green-status readings until minutes before the crash. The asset was not failing. Then it was destroyed."

The dashboard did not fail. The sensors did not fail. The monitoring system performed exactly as designed. The problem is not a malfunction — it is an architectural limitation built into the foundation of every amplitude-based monitoring system currently deployed in industrial operations.

1.1 How Threshold Monitoring Actually Works

Standard industrial monitoring establishes a baseline operating range for measured parameters and triggers an alarm when a reading crosses a predefined limit. This architecture has one critical structural flaw: it cannot fire until the damage has already begun. Consider bearing fatigue. A bearing does not fail in a single moment. The failure process begins weeks or months earlier with sub-surface micro-fractures that produce no detectable vibration amplitude change — the bearing rotates smoothly, within spec. As the micro-fractures propagate, they alter the information structure of the vibration signal long before they alter its amplitude. Standard monitoring cannot see this.

1.2 The Lagging Indicator Problem

Vibration, temperature, and pressure are all lagging indicators of mechanical health. They measure the observable consequences of physical processes, not the processes themselves. By the time a monitored signal breaches a threshold:

- The underlying structural damage has already propagated beyond preventable limits.
- The maintenance window is reactive — emergency response rather than scheduled intervention.
- Secondary damage to adjacent components has frequently already begun.
- The "predictive" maintenance program is, in practice, a reactive one with faster response times.

Monitoring Approach	What It Measures	When It Fires	Nature
Threshold Alarm	Signal amplitude	After threshold breach	Lagging — reactive
Rule-Based Systems	Predefined conditions	After condition met	Lagging — reactive
Statistical ML	Pattern correlation	When pattern matches training data	Lagging + requires training data

UIP Framework	**Signal structural integrity**	**Weeks/months before amplitude breach**	**Leading — predictive**

Table 1.1 — Monitoring Approach Comparison: Leading vs. Lagging Indicators

2.0 KNOWN FAILURE MODES OF STATISTICAL APPROACHES

The limitations of amplitude-based monitoring are well understood. The industry response has been to deploy machine learning and statistical anomaly detection. These approaches improve on static threshold alarms but carry a different and frequently underestimated set of failure modes.

2.1 The Training Data Dependency

- **Sparse failure history.** Most industrial operations do not have large libraries of labeled failure events. The training corpus for a meaningful ML model rarely exists.
- **Novel failure mode blindness.** An ML model trained on bearing fatigue patterns will not recognize hydraulic crystallization. If the failure mode was not in the training data, the model is blind to it.
- **False confidence from false negatives.** An ML model's silence is frequently interpreted as a clean bill of health. It only confirms that no previously observed failure pattern has been matched — not that the asset is healthy.

2.2 The Probabilistic Black Box Problem

Standard ML anomaly detection operates through statistical inference. When the model flags an anomaly, it cannot explain the physical mechanism causing it. When it fails to flag an anomaly, it cannot explain why. A system that cannot explain its detections cannot be trusted by an engineer whose professional judgment will be called upon to act on them.

> **FSME Logic's position:** Deterministic physics is auditable. Statistical pattern-matching is not. An engineer must be able to understand why an alert was generated — not simply that a probability threshold was crossed.

3.0 THE UNIFIED INFORMATION POTENTIAL FRAMEWORK

UIP is a physics-based signal integrity framework grounded in advanced time-series behavioral memory and information theory. It does not predict failure by recognizing patterns. It predicts failure by measuring the physical degradation of a signal's structural properties.

3.1 Structural Coherence States

A healthy mechanical or electronic system generates output signals with a characteristic property: they breathe. The signal fluctuates, varies, and maintains a complex dynamic equilibrium reflecting the system's internal degrees of freedom — thermal motion, micro-adjustments of rotating components, pressure fluctuations of fluid dynamics. This quality is called **structural coherence state**.

As a system degrades, it progressively loses this elasticity. The signal becomes constraineder, more predictable, more repetitive. The system is, in a measurable physical sense, crystallizing toward failure. Its output signal carries less information about a healthy dynamic state and more information about a constrained, damaged one.

> Imagine a healthy vibration signal: dynamically variable, structurally rich. A degrading signal exhibits a constrained dynamic footprint — the signal loses its structural complexity before it loses its function. **FSME reads this change directly.**

3.2 Sequential State Dependency

Standard signal processing typically treats each measurement as statistically independent — the Markovian assumption that the current state contains no information about past states. This is mathematically convenient but physically false for mechanical systems under stress. Real mechanical systems have memory. A bearing that experienced an overload event three days ago is not in the same state as an identical bearing that did not. The stress history of the system is encoded in the statistical structure of its output signals. UIP operates within a advanced time-series behavioral memory framework that explicitly accounts for this memory.

3.3 The High-Level Framework

UIP operates on three measurable properties of the signal:

- **Signal Coherence States:** How much structural information is present per unit time. A healthy system maintains high information density. A degrading system exhibits falling density as the signal becomes more constrained.
- **Temporal Degradation Mapping:** How long the signal maintains longitudinal state continuity. Healthy systems exhibit long-memory persistence. Degrading systems show progressive memory loss as the physical mechanisms sustaining that persistence are damaged.
- **Kinematic Entropy Profiles:** The characteristic rate at which the signal's information properties change. Pre-failure degradation produces characteristic changes in volatility that are detectable

before any amplitude threshold is breached.

Proprietary Boundary. The specific implementation of the UIP framework — including kernel functions, detection operators, calibration parameters, and computational architecture — is the proprietary intellectual property of FSME Logic, protected under pending Canadian Patent Application CA 3,297,487. Implementation details are not disclosed in this document. The framework above describes what is measured, not how the measurement is computed.

4.0 CROSS-DOMAIN VALIDATION SUMMARY

The FSME engine was benchmarked against publicly available datasets spanning four distinct physical domains. No domain-specific retraining, parameter adjustment, or specialized configuration was applied when transitioning between domains. The consistent detection performance across these domains is the primary empirical evidence for the universality of the UIP physical framework.

All validation datasets cited below are publicly available and independently verifiable.

4.1 Industrial Machinery

Dataset	Domain	FSME Detection Result
Standardized Industrial Rotating Machinery Benchmark (Case Univ.)	Ball bearings Rotating machinery	Pre-failure signature detected across all 9 fault types at 3 severity levels before amplitude deviation was observable
Accelerated Run-to-Failure Industrial Bearing Repository	Industrial bearings (run-to-failure)	Consistent pre-failure detection with lead times of 1.1 to 7.6 hours before physical failure event
UCI Hydraulic System Condition Monitoring Dataset	Hydraulic systems (pressure, flow, temp)	Degradation detected up to 160 operating cycles before standard condition thresholds would have triggered

Table 4.1 — Industrial Machinery Validation

4.2 Aerospace and Space Systems

Dataset	Domain	FSME Detection Result
Tier-1 Aerospace Turbofan Fleet Telemetry (509 engines)	Aerospace propulsion (509 engines)	78% fleet-wide detection rate with an average predictive lead time of 126 operating cycles before end-of-life
Deep-Space Robotics Actuator Telemetry Archive	Space robotics Actuator systems	Pre-failure signature detected 6.3 hours before actuator binding reached detectable amplitude — vs. minutes warning from standard monitoring
Orbital Spacecraft Anomaly Detection Archive	Orbital spacecraft Telemetry systems	Consistent multi-channel pre-anomaly detection across benchmark test cases without domain-specific tuning

Table 4.2 — Aerospace and Space Systems Validation

4.3 Quantum Hardware and Fundamental Physics

These tests were designed to probe whether UIP is detecting a genuine physical phenomenon or an artifact specific to industrial signal characteristics.

Dataset	Domain	Finding
Fundamental Physics Deep-Space Strain Baselines	Fundamental physics GW detection	UIP identified the same class of structural signature changes in gravitational wave strain data as in industrial vibration signals. The measured physical property is domain-agnostic.
Superconducting Qubit Decoherence Calibration Logs	Quantum hardware Superconducting qubits	Kinematic signature degradation consistent with those in industrial degradation observed in quantum decoherence data, confirming the framework's universality across physical scales.
Astrophysical Timing Residue Archive	Radio astronomy Pulsar timing	Signal memory and structural volatility metrics consistent with UIP predictions observed in pulsar timing noise profiles.

Table 4.3 — Quantum and Fundamental Physics Validation

The Gravitational Flex. If the UIP framework can isolate structural degradation signatures in gravitational wave strain data — the most noise-contaminated, physically extreme dataset in modern science — detecting sub-surface bearing fracture in a 2,000 RPM industrial gearbox is, by comparison, a direct application of the same underlying physics.

5.0 COMPARATIVE ADVANTAGE

5.1 No Training Data Required

FSME Logic requires no historical failure data. The UIP framework derives its detection capability from the physics of signal degradation, not from learned associations between signal patterns and labeled failure events. The same parameters that detect bearing fatigue detect hydraulic crystallization, actuator binding, and quantum decoherence — because the underlying physical phenomenon is the same.

5.2 Fully Offline, Air-Gapped Capable

Many industrial, defense, and critical infrastructure environments cannot send proprietary telemetry data to third-party cloud servers. The FSME engine runs completely offline on local hardware with no internet dependency, no API calls, no telemetry transmission, and no cloud processing. License activation is manual and does not require a network connection. Every competitor in the predictive maintenance space that requires cloud connectivity cannot serve this client segment.

5.3 Capability Summary

Capability	Threshold Alarm	ML Anomaly Detection	UIP Framework
Fires before physical damage	No	Sometimes	**Yes**
Requires training data	No	Yes — labeled dataset required	**No**
Detects novel failure modes	No	No — blind to unseen patterns	**Yes**
Operates fully offline	Yes	Usually not	**Yes**
Explains detection cause	Threshold exceeded	No — probabilistic	Yes — physical mechanism
Cross-domain without retraining	No	No	**Yes — 4 domains validated**

Table 5.1 — Capability Comparison

5.5 THE CYBERSECURITY BURDEN OF PREDICTIVE ANALYTICS

The manufacturing and industrial sectors have become the most aggressively targeted industries for cyberattacks globally, surpassing financial services and healthcare. The primary attack vector in the majority of industrial incidents is the exploitation of public-facing applications — software systems that require constant internet connectivity to function. Every cloud-based predictive maintenance platform deployed in an industrial environment represents exactly this kind of publicly accessible attack surface.

> **FSME Logic architectural response:** Unlike cloud-based anomaly detection platforms that require continuous public-facing internet connections, the FSME Predictive Integrity Engine operates entirely offline. There are no public-facing applications. No remote external services. No API endpoints exposed to the web. The engine runs on isolated edge hardware with full-disk encryption and zero open router ports. Supply chain compromise through third-party cloud integrations is architecturally impossible — because there is no supply chain to compromise.

For defense contractors handling export-controlled (ITAR) or Controlled Unclassified Information (CUI) telemetry, the FSME architecture satisfies zero-trust requirements by default. There is no data egress. No third-party data processor. All analysis occurs on founder-operated hardware in Edmonton, Alberta, Canada — a single, verifiable, air-gapped environment.

6.0 OPERATIONAL BOUNDARIES

A method claiming universal applicability without qualification either oversells its capabilities or has not been tested enough to discover its limits. The following boundaries define where UIP is and is not expected to perform reliably.

6.1 Conditions Required for Reliable Detection

- **Sensor fidelity:** The monitoring system must capture the signal with sufficient temporal resolution to observe the structural properties UIP relies on. Very low sample-rate sensors on fast-rotating equipment may not capture the relevant signal characteristics.
- **Minimum observation window:** UIP requires sufficient signal history to establish a structural baseline. Datasets under 30 days of continuous operation may not provide adequate context.
- **Physical observability:** The failing component must be accessible to a monitored sensor. If no sensor can observe the degradation, no monitoring system can detect it.
- **Signal coherence:** Signals with severe external corruption — electrical interference, damaged cables, intermittent connections — may produce structural changes indistinguishable from degradation signatures. Data quality review is a prerequisite.

6.2 Conditions Where Alternative Methods May Be Preferred

- **Narrow, recurring fault classification:** Operations with extensive labeled historical data for a specific recurring fault mode may find supervised ML classification faster for that single specific task.
- **Millisecond-latency control loops:** UIP is a forensic analysis tool, not a real-time closed-loop control input. Applications requiring sub-millisecond response should use purpose-built real-time systems.

> Defining where a method does not work is not a weakness. It is the mark of engineering discipline. FSME Logic does not oversell.

7.0 THE FSME FORENSIC AUDIT PROCESS

The FSME engine is delivered as a forensic audit service. The client provides raw historical telemetry. FSME Logic processes it on air-gapped hardware and returns a structured forensic report. There is no software to install, no API to integrate, no cloud account to provision, and no training phase to complete.

7.1 What You Need

- **Time-series sensor data** in any supported format (.csv, .h5/.hdf5, .tdms, .nc, .mat, .xlsx, .json, .sqlite, .parquet)
- **Minimum 30 days** of continuous operational data; 60–90 days is optimal
- **All available sensor channels** for the target asset — pre-filtering is discouraged
- For Viability Assessments: the approximate **date of the historical failure event** being assessed

7.2 The Engagement Process

#	Step	Detail
1	Compatibility check	Client describes equipment type and data volume. FSME Logic confirms compatibility.
2	NDA (if required)	Mutual NDA executed before any data exchange.
3	Secure transfer	Client transfers raw telemetry via encrypted email, secure file transfer, or physical media. No public cloud involved.
4	SHA-256 receipt	FSME Logic sends a SHA-256 hash of the received file within 24 hours, confirming intact receipt.
5	Air-gapped analysis	Analysis runs on dedicated offline hardware in Edmonton. No internet connection used during processing.
6	Report delivery	Forensic PDF delivered by encrypted email. Typical turnaround: 3–7 business days.
6.5	Expert interpretation	Structural analysis arrays are reviewed and interpreted by FSME Logic to generate the final capital impact report and detection timeline. The forensic PDF reflects expert contextualisation of the engine output, not raw algorithmic data.
7	Data destruction	Raw data files securely deleted following delivery. Confirmed in writing on request.

Table 7.1 — FSME Logic Forensic Audit Engagement Process

7.3 The Single-Asset Viability Assessment

The Viability Assessment is the standard entry point. The client provides telemetry from one historical failure event. FSME Logic analyzes it and produces a forensic report demonstrating whether UIP would have detected the pre-failure signature before the standard monitoring system triggered.

> **Guarantee:** If the UIP framework cannot mathematically demonstrate a predictive detection window prior to the client's SCADA alarm trigger on the provided historical dataset, the $999 CAD assessment fee is refunded in full. Automatic. No conditions.

7.4 Forensic Report Contents

- **Executive Financial Summary:** Translation of the failure event into capital impact — actual downtime cost, repair cost, and what the predictive lead time would have been worth operationally.
- **Detection Timeline:** Chronological plot showing when UIP first detected the pre-failure signature vs. when standard monitoring alarmed.
- **Channel-by-Channel Analysis:** Identification of which sensor channels carried the earliest detectable signature and the progression of degradation.
- **Fleet-Wide Extrapolation:** Statistical projection of similar unmonitored stress accumulations across the client's remaining asset fleet.
- **SHA-256 Chain of Custody:** Cryptographic documentation that the data was processed on isolated hardware and not transmitted over any public network.

8.0 PRIORITY STATEMENT AND IP BOUNDARY

8.1 Development Timeline

The UIP theoretical framework was formalized and documented in December 2025. Experimental validation on benchmark datasets followed in January 2026. Theory first. Experimental confirmation second. The results were predicted, not retrofitted. Canadian Patent Application CA 3,297,487 was filed in December 2025.

8.2 What This Document Discloses

- The physical quantities UIP measures — signal structural integrity, structural coherence state, non-Markovian memory persistence
- The conceptual framework — what the engine does, not how it is implemented
- Validation results on publicly available benchmark datasets
- The engagement and delivery process

8.3 What This Document Does Not Disclose

The following information is proprietary to FSME Logic and protected by Patent CA 3,297,487. It is not disclosed in this or any public document: • Specific mathematical kernel functions and detection operators • Internal calibration parameters and derived constants • Computational architecture of the detection pipeline • Any element of the source code or algorithm implementation The FSME engine is delivered as a compiled binary for forensic audit engagements. No source code, parameters, or proprietary implementation details are accessible to clients.

8.4 Reproducibility

All validation datasets cited in this document are publicly available. The benchmark results described — detection lead times, fault classification rates, cross-domain performance — can be independently verified by any researcher with access to the same public datasets. FSME Logic does not assert results that cannot be independently validated against public data.

9.0 FORMAL DEFINITIONS

The following terms are used with specific, technical meaning throughout this document. Where terms have been introduced by FSME Logic, the definition given here is authoritative.

Green Dashboard Fallacy	A systemic false-positive confidence condition in which monitoring metrics indicate nominal operation while latent physical failure conditions are actively accumulating in the monitored asset. Named for the visual pattern of all-green SCADA displays observed immediately before catastrophic failures.
Unified Information Potential (UIP)	A physics-based scalar quantity that characterizes the structural integrity of a time-series signal by measuring properties related to information density, memory persistence, and structural coherence state. Specific implementation details are proprietary.
Structural Coherence States	The property of a healthy system's output signal characterized by maintained baseline operational variance. A quantitative measure of the signal's capacity to carry information about the system's healthy dynamic state. Progressive loss of structural coherence state is the primary physical indicator of sub-threshold degradation.
Non-Markovian Dynamics	A class of physical systems in which the present state carries measurable information about past states. Contrasted with Markovian systems where each state is statistically independent of prior states. Real mechanical systems under stress exhibit non-Markovian behavior.
Kinematic Signature Degradation	The measurable breakdown of structural coherence state preceding mechanical failure. Characterized by progressive signal constrainedening, reduced information density, and loss of memory persistence. The primary phenomenon the FSME engine is designed to detect.
Lagging Indicator	A measurement reflecting the consequences of a physical event after it has already occurred. Standard amplitude threshold alarms are lagging indicators. They report that a threshold has been breached; they cannot predict when a threshold will be breached.
Predictive Integrity Engine	The compiled FSME Logic implementation of the UIP framework. Delivered as an air-gapped binary for forensic audit engagements. Implementation details are proprietary.
Proprietary Data Ingestion Protocol	An FSME data ingestion methodology that reconstructs a drift-free, uniformly spaced time axis from sensor data with missing samples, variable sample rates, or corrupted timestamps.

10.0 CONCLUSION AND THE DATASET CHALLENGE

10.1 Summary

Standard industrial monitoring is structurally limited to detecting the amplitude consequences of mechanical failure. It cannot detect the physical processes that cause those consequences before they produce amplitude changes. This is not solvable within the amplitude-monitoring paradigm.

The UIP framework addresses this gap by measuring signal structural integrity. These properties degrade measurably before amplitude thresholds are breached. The framework has been validated across industrial machinery, aerospace propulsion, orbital spacecraft, Mars surface robotics, gravitational wave observatories, and quantum computing hardware — with consistent detection performance in every domain and without domain-specific retraining.

10.2 When to Consider a Forensic Audit

- Assets where a single unplanned failure costs more than $5,000 CAD in repair and downtime
- Operations where historical failure data is sparse, making ML-based approaches impractical
- Facilities with IT or security constraints preventing cloud analytics deployment
- Equipment that has experienced unexpected failures with no advance warning from standard monitoring

10.3 The Dataset Challenge

The theoretical limits of deterministic physics cannot be fully appreciated through benchmark data alone. They must be observed on your own assets. Do not send clean data. Export the telemetry from your ugliest, most complex historical failure — the one where the dashboard was green until the asset was destroyed. Submit it for a Single-Asset Viability Assessment. If the UIP framework cannot mathematically demonstrate a predictive detection window prior to your SCADA alarm trigger, **the $999 CAD fee is refunded in full. Automatically. No conditions.** Contact: alex-kalyniuk@fsmelogic.ca | fsmelogic.ca/store.html#viability-assessment

FSME Logic | Edmonton, Alberta, Canada | alex-kalyniuk@fsmelogic.ca | fsmelogic.ca

EXECUTIVE ROI SUMMARY

— Print this page and hand it to your VP of Maintenance to secure approval for the Viability Assessment —

The Problem

Current vibration, thermal, and SCADA monitoring systems are amplitude-based. They fire when damage has already occurred. The majority of catastrophic industrial failures occur with no advance warning from standard monitoring. This is an architectural limitation of threshold-based monitoring — not a malfunction.

What Is Being Requested

Item	Detail	Cost
Single-Asset Viability Assessment	FSME Logic analyzes historical telemetry from one asset failure. Proves whether sub-surface degradation was detectable before your standard alarm triggered.	$999 CAD
Financial Risk	Automatic full refund if early detection cannot be demonstrated.	$0 risk
Infrastructure Required	None — no software install, cloud account, API integration, or new hardware.	$0
Data Security	Air-gapped processing. SHA-256 custody receipt. Data destroyed after delivery. No cloud. No third-party.	Full sovereignty
Credit Toward Fleet Audit	$999 credited in full toward any subsequent fleet-wide engagement.	$999 credit

A single unplanned failure event on a hydraulic system, gearbox, or compressor typically costs $15,000 to $150,000 in emergency repair, downtime, and secondary damage. This assessment costs $999 with a full refund guarantee. The risk-adjusted expected value of approving this expenditure is strongly positive.

Validation Credentials

Benchmark	Result
a Tier-1 Aerospace Turbofan Fleet Telemetry archive (509 turbofan engines)	78% fleet detection rate — 126-cycle avg. predictive lead time
NASA Mars Curiosity Rover actuator	6.3-hour warning before actuator binding failure
Standardized Industrial Bearing Benchmark	Detection across 9 fault types, 3 severity levels
4 physical domains validated	Industrial, aerospace, gravitational wave, quantum — same engine, no retraining

To initiate: alex-kalyniuk@fsmelogic.ca | fsmelogic.ca/store.html#viability-assessment | Proprietary & Trade Secret Protected