General Framework for Integrated Biological, Material, and Instrument Data (G-FIBMID): A Degradation-Aware Cyber-Physical State Architecture for Cyberbiosecure Biological Systems in Extreme Environments

Guillermo Bojorge[1][1], Sotirios F. Karathanasis[2], Celisha Oscar[3], Indrani Ghosh Dastider[4], Diganta Dutta[5][2]Lucas Potter[6] and Xavier-Lewis Palmer[6]

[1]Independent Researcher, CA, USA
[2]Independent Researcher, USA
[3]Howard University, D.C., USA
[4]University of Nebraska Medical Center, NE, USA
[5]University of Nebraska at Kearney, NE, USA
[6]Biosview Labs, OH, USA

duttad2@unk.edu (Corresponding author)
gmobojorge@gmail.com (Corresponding author)
biosview1@proton.me (Corresponding author)

Abstract: It is not a given that we can trust all data obtained from space-based experiments without understanding how deterioration on hardware may influence said data. Space exerts known deleterious effects on hardware stability. This is a mission-critical problem for data handling and storage in scientific missions. Biological experimentation in extreme environments and contexts such as orbital platform usage, deep-space missions, and high-radiation terrestrial facilities, relies on instrumentation that is sensitive to radiation exposure, mechanical fatigue, thermal cycling, and configuration drift. Existing bioimaging and bioscience metadata and provenance frameworks provide mechanisms for documenting acquisition settings, experimental context and data lineage (Goldberg et al., 2005; Sansone et al., 2012; W3C, 2013). This paper proposes additional time-indexed linkage to an explicit model of evolving instrument condition. As a consequence, it is difficult to determine with confidence whether results are due to real biological changes or due instrument degradation. This introduces interpretive ambiguity into mission-critical scenarios, becoming a cyberbiosecurity risk. This vision paper presents a framework provisionally titled: General Framework for Integrated Biological, Material, and Instrument Data (G-FIBMID), a degradation-aware digital twin architecture that formalizes hardware evolution as a first-class, cryptographically-secured provenance variable. The framework has the Degradation State Vector as its center, which is a structured and time-indexed representation of cumulative physical wear, operational fatigue, configuration changes, and environmental exposure. Under G-FIBMID, biological measurements would be cryptographically associated with corresponding, time-indexed Degradation State Vector (DSV) snapshots through a secure Provenance Linkage Layer, with the aim of supporting bias estimation, anomaly investigation, and auditable autonomous workflows under mission constraints; these capabilities remain to be validated. In order to demonstrate a practical instance of this framework, a ground-to-flight Atomic Force Microscope (AFM) scenario is explored to demonstrate its utility while preserving instrument-agnostic generality. G-FIBMID proposes to transform hardware drift from an unobserved confounder into a measurable and securable dimension of biological interpretation by integrating reliability modeling, secure telemetry capture, and lifecycle-aware correction workflows. The goal of this architecture is to advance cyberbiosecurity by protecting both data integrity and the continuity of biological meaning in extreme environments where instrument condition and biological systems evolve under sustained operational stress.

Keywords: Cyberbiosecurity, Data provenance, Hardware degradation, Deep-space missions, Secure telemetry

1. Introduction and Problem Framing

Biological experiments in space and high-radiation facilities use instruments exposed to physical and computational stresses. Radiation, vibration and thermal cycling can alter instrument performance; radiation-induced single-event upsets can also affect digital memory and logic (Dodd and Massengill, 2003). Established bioscience frameworks record sample context, acquisition metadata and data lineage (Goldberg et al., 2005; Sansone et al., 2012; W3C, 2013), yet an authenticated history of instrument condition is not always linked to each measurement. This concern intensifies during autonomous missions: ionizing radiation can disrupt microelectronics (Dodd and Massengill, 2003), while preserving stored information poses different challenges

[1]Guillermo Bojorge and Sotirios F. Karathanasis (*Shared First-authorship)*

[2]Diganta Dutta, Lucas Potter and Xavier-Lewis Palmer (*Shared Last-authorship)*

(Rosenthal, 2010). Figure 1 illustrates manual file-byte corruption, not experimentally reproduced radiation damage.

A recorded biological signal may reflect both the sample and its changing measurement apparatus. Probe wear, optical drift, actuator creep, configuration changes and telemetry errors can resemble biological responses. When measurement histories omit these changes, investigators may misattribute variation, particularly where results inform microbial monitoring, life support or crew diagnostics. Physical deterioration and adversarial actions must also be distinguished: corrupted telemetry or altered calibration records may compromise interpretation without any alteration of the sample. Degradation histories can therefore serve two related functions: documenting measurement uncertainty and providing evidence for cyber-physical integrity checks. They do not, on their own, prove measurement accuracy or identify the cause of a deviation.

G-FIBMID proposes treating time-resolved instrument condition as a provenance variable secured alongside biological observations. It connects degradation-state modeling, predictive instrument twins and verifiable records so investigators can ask whether an apparent biological change could instead reflect instrument behavior. The framework is conceptual; empirical calibration and a defined threat model are necessary before claims of corrected or trustworthy biological interpretation can be demonstrated. See Appendix for Supplementary Figure A that defines the terminology.

1.1 Vision Framing

At microscale and nanoscale resolutions, relatively small changes in instrument behavior may produce measurement artifacts that complicate the distinction between biological responses and hardware-induced variation. Atomic force microscopy exemplifies how mechanical stability, probe condition and calibration influence measurement uncertainty (Eaton and West, 2010; Klapetek et al., 2011; Sullan et al., 2013). The broader applicability to nanopore sequencing, lab-on-chip platforms and flow cytometers remains an instrument-specific proposition requiring corresponding primary evidence. The importance of identifying changes over repeated use, and implementing those changes in final study data depots can enhance transparency and ease of replication across research teams. While the physical stressors to equipment can be attenuated through engineering breakthroughs, quality control and improvements to scientific instrumentation, studies in the past have attempted to use adaptive learning models. In 2024, Sokolov and colleagues explored whether machine learning (ML) could be used to assist AFM micrograph classification, identification, and analysis for medical and materials science purposes (Sokolov, 2024). Petrov et al. (2024) demonstrated machine-learning-assisted identification of materials using nanoscale AFM mechanical-property maps; this establishes an analytical use of high-resolution instrument data rather than a degradation-state model. Machine-learning methods have been applied to high-dimensional cytometry data analysis and cell-population classification (Hu, Bhattacharya and Butte, 2022); that review does not directly demonstrate correction of physical cytometer misalignment. Märtens et al. (2023) developed Rarity, a framework for detecting rare cell populations in imaging mass cytometry data; this demonstrates the importance of interpreting subtle marker-expression patterns but does not evaluate instrument degradation. These examples motivate investigating how a mathematically specified degradation model might complement existing image and cytometry analysis; they do not establish that such a model has already been validated. While this sets to enhance study congruency, it solidifies the confidence in research teams concluding what is hardware influence, and what is a biological phenomenon.

1.2 Methodological Framework

To systematically model hardware evolution as a first-class provenance variable, this paper constructs a conceptual, architectural, and evaluative framework structured across five core methodological phases. These are:

1. Cyberbiosecurity & Interpretive Risk Framing: We integrate cyberbiosecurity threat modeling (Murch et al., 2018; George, 2019; Potter and Palmer, 2023) with cyber-physical system security (Crawford et al., 2023; Dove et al., 2025) to formalize how hardware drift, telemetry corruption, and unmodeled sensor degradation introduce systematic interpretive bias in extreme environments.
2. Degradation State Vector (DSV) Formalization & Mathematical Abstraction: We establish the Degradation State Vector (DSV) as a time-indexed mathematical abstraction quantifying cumulative radiation dose, operational fatigue, sensor/actuator drift, thermal exposure, and configuration evolution. AFM measurement stability and artifacts have been studied experimentally (Sullan et al., 2013; Gołek et al., 2014), and radiation effects on certain piezoelectric sensors have been reported (Haider et al., 2019). Established prognostics guidance from the International Organization for

Standardization (ISO, 2025) and digital-twin research (Tao et al., 2019) motivate comparison of observed and predicted state trajectories; this manuscript proposes the ΔDSV comparison without presenting empirical validation.

3. Cryptographic Lineage & Root-of-Trust Integration: We design a multi-layered security architecture consisting of: a. Layer 1 (Biological Measurement Events): Encapsulating sample data, environmental parameters, and temporal metadata. b. Layer 2 (Digital Twin & DSV Engine): Continuously logging hardware parameters and operational states. c. Layer 3 (Provenance Linkage Layer): Cryptographically binding Layer 1 measurements to Layer 2 state snapshots using hardware root-of-trust signatures, secure time authority, and append-only tamper-evident chaining (Regenscheid, 2018; Laurie, Messeri and Stradling, 2021; Birkholz et al., 2023).
4. Demonstrative Case Study (Ground-to-Flight Atomic Force Microscopy): To illustrate architectural applicability, we synthesize physical degradation mechanics in high-precision micro/nanoscale instrumentation (Voigtländer, 2019). Drawing on documented spaceflight AFM heritage (Rosetta MIDAS and Phoenix Mars Lander MECA; Riedler et al., 2007; Hecht et al., 2008), we model nanomechanical failure modes including probe tip wear and deformation (Chen et al., 2004; Chen, 2012; Chen et al., 2019; Orji et al., 2020), piezoelectric hysteresis, cantilever fatigue, and laser thermal drift (Eaton and West, 2010; Klapetek et al., 2011, 2024; Sadewasser et al., 2018). Proposed schemas would draw on established OME acquisition metadata and interoperable imaging formats; the specific DSV serialization and AFM mappings require definition (Goldberg et al., 2005; Moore et al., 2021).
5. Autonomous Correction & Machine Learning Integration: We structure adaptive correction workflows drawing on research in AFM image processing and machine learning (Erickson et al., 2012; Sokolov, 2024; Dickbreder et al., 2023) to explore whether instrument-related artifacts could be estimated and corrected. Performance in autonomous deep-space deployments remains an evaluation objective.

Together, these five structured phases establish a comprehensive methodology for moving beyond conventional static metadata models. By systematically integrating hardware degradation tracking with cryptographic verification, the proposed framework aims to improve the robustness, traceability, and interpretability of data provenance throughout extreme-environment missions, subject to empirical validation.

2. Degradation as a First-class Provenance Variable

Established provenance models describe acquisition context and data lineage (Goldberg et al., 2005; W3C, 2013). G-FIBMID investigates whether biological measurements should also be explicitly linked to authenticated, time-varying estimates of instrument condition. Degradation may accumulate through use or exposure, occur abruptly after shock, or accompany firmware and calibration changes. Relevant indicators include drift, fatigue, dose and probe condition (Sullan et al., 2013; Gołek et al., 2014).

We define the Degradation State Vector (DSV) as an instrument-specific, time-indexed record of measured or estimated condition variables. The DSV is a multicomponent representation rather than a single physical quantity; component units, uncertainty, baselines, sampling intervals and validation requirements must be specified for each instrument. Different mission phases, including preflight, launch, mission operations, and descent where applicable, may require distinct instrument-degradation models. If degradation-related bias can be calibrated independently, DSV information could help estimate its contribution to a biological signal. Without such calibration, it can flag uncertainty but cannot legitimately subtract an artifact or certify biological validity.

Degradation histories are also security-relevant because altered firmware, missing calibration events or truncated logs can obscure how a measurement was obtained. Hardware-protected keys, trusted timestamps and tamper-evident records could make unauthorized changes more observable, subject to the system's trust assumptions. A digital twin would estimate the instrument's expected state using validated models. Define the state residual as $\Delta DSV(t) = DSV_observed(t) - DSV_predicted(t)$, with compatible components and aligned time points; it is a vector difference, not a vector product. Unexpected residuals would prompt investigation, not automatically indicate attack. Existing scanning-probe drift-correction work (Dickbreder et al., 2023) motivates instrument-specific correction research but does not validate a DSV digital twin. This distinction places G-FIBMID's proposed novelty in the secure measurement–state association rather than in the prior existence of drift correction or digital twins.

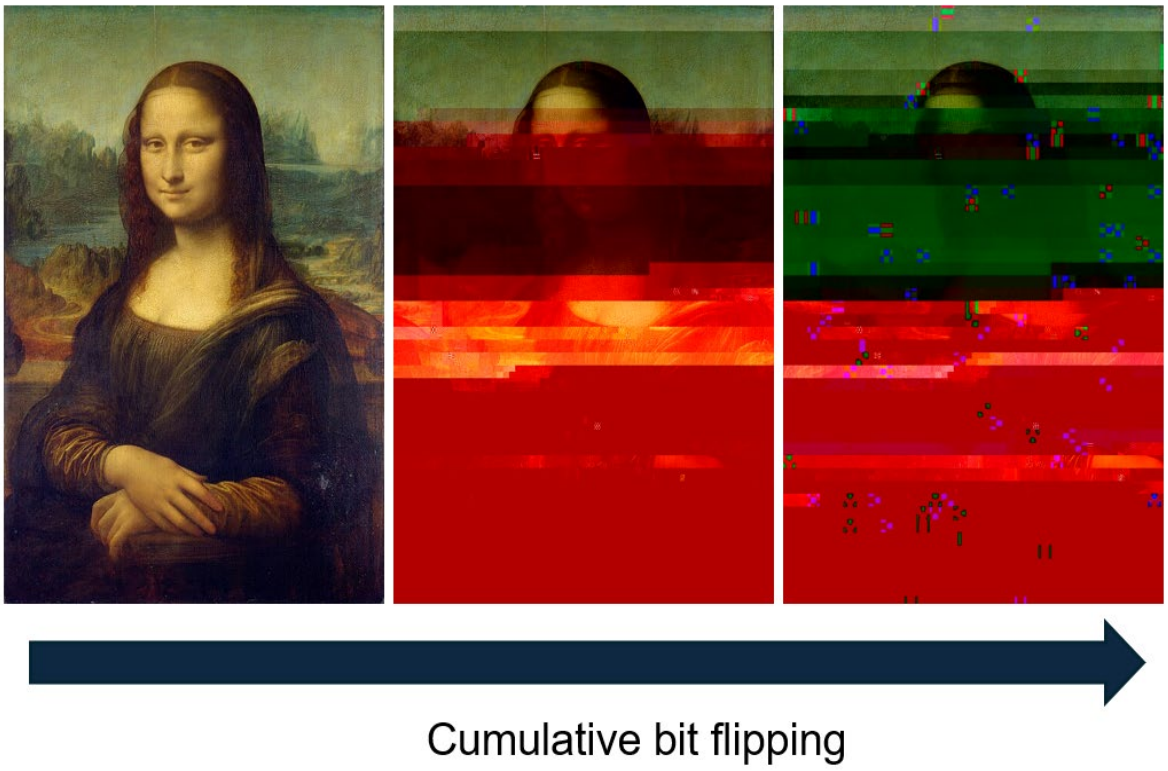

Figure 1: Illustrative effects of cumulative bit alterations on digital image integrity. A public-domain digital reproduction of Leonardo da Vinci's Mona Lisa, sourced from the Musée du Louvre via Wikimedia Commons (Wikimedia Commons, n.d.), was opened using HxD Hex Editor, version 2.5.0.0 (Hörz, 2021). Individual bits were manually inverted (0 to 1 or 1 to 0), cumulatively from left to right. By the fourth alteration, the file became corrupted and unusable. This demonstration illustrates digital file corruption rather than experimentally reproduced radiation damage; its failure threshold should not be generalized to spacecraft memory systems

3. G-FIBMID Architecture

G-FIBMID links each biological observation to an authenticated record of instrument condition at acquisition. Its digital twin predicts instrument-specific degradation trajectories for comparison with the observed DSV. Deviations could trigger review or inform bias estimation where validated calibration models exist. A predicted degradation state alone cannot establish the amount of measurement bias or justify subtracting it from raw biological data.

The proposed architecture contains three layers.

- Layer 1, Biological Measurement Events, holds sample data, experimental conditions, timestamps and a reference to acquisition state.
- Layer 2, Digital Twin and DSV Engine, records operational parameters, calibration history, firmware configuration, environmental exposure and predicted-versus-observed condition.
- Layer 3, Provenance Linkage Layer, binds measurements to authenticated state snapshots and the telemetry window used to interpret them. Signing supports record integrity but does not independently verify sensor accuracy.

For the purposes of demonstrating the value of the DSV, we use atomic force microscopy (AFM) and its use in deep space as a particularly sensitive example. Atomic Force Microscopy (AFM) is an imaging technique that scans a sharp, nanoscopic probe over a surface to measure cantilever deflections, using quantitative imaging to generate high-resolution maps of surface topography and mechanical properties such as stiffness, adhesion, and elasticity. AFM probes sample surfaces at micro- to nanoscales, with achievable resolution depending on the probe, operating mode and specimen (Voigtländer, 2019). Machine-learning-assisted AFM mechanical spectroscopy can illustrate how inferred material identities depend on instrument-derived property maps (Petrov et al., 2024). AFMs are highly sensitive to physical perturbations at the nanometer-scale, thus even

subtle changes such as mechanical drift, piezoelectric hysteresis, cantilever fatigue, thermal expansion, or calibration variability can introduce errors; making AFM a suitable illustrative case for degradation-aware provenance (Klapetek et al., 2011, 2024; Nečas and Klapetek, 2017; Sadewasser, Nicoara and Solares, 2018). Beyond these physical perturbations, even minute deviations from pretesting quality assurance can cause gross changes in data (Eaton and West, 2010; Chen et al, 2004; Chen, 2012; Chen et al., 2019): overextended operation, actuator creep, laser sway, cantilever tip conformational changes (Figure 2), cantilever block frosting, spring constant deviation and thermal drift can alter measured force–distance curves. Without structured modeling of instrument use-evolution, observed changes could be misinterpreted as biological adaptation rather than hardware drift. Among these factors, operational fatigue is particularly significant in AFM research when utilizing the same cantilever across multiple trials of an experiment. Repeated use of an AFM cantilever may contribute to probe tip wear, potentially affecting measurement accuracy and consistency (Orji et al., 2020). The extent to which a cantilever can be reused depends on the specimen, probe characteristics, operating conditions, and experimental protocol.

Under the proposed architecture, each DSV update would be digitally signed using a hardware-backed root of trust and linked to preceding records. Under the proposed architecture, each biological measurement would be cryptographically associated with the corresponding DSV snapshot recorded at acquisition. Revisiting our AFM example, information cataloged in an instrument's snapshot should include cantilever-specific parameters including cantilever model, spring constant, frequency, z-speed, z-length, calibration coefficient, media, and laser signal return from each individual cantilever. Whole-instrument metadata would record the AFM model and serial number, piezo position, and relevant environmental variables, such as temperature, relative humidity, atmospheric pressure, ultraviolet irradiance, and gas composition (e.g., O_2, CO_2, and N_2 volume fractions), where measured. Units and acquisition timestamps would accompany each recorded variable. Interpretation therefore becomes dependent on the verified hardware state. This linkage allows measurement interpretation to incorporate authenticated instrument-state information alongside biological metadata, although authentication alone cannot establish measurement accuracy. Staying in this vein, DSVs can be implemented as part of a broader validation schema in order to compare two or more instruments making the same measurements; these instruments could be the same (comparing instruments of the same model, or those that are expected to operate similarly but are housed in different locations), different versions of the same machine (version 1 vs. version 2), or machines from different manufacturers. The collection of this data also can be maintained in an organized fashion locally on the machine: state variables used in building the DSV can be easily included with raw data either by being appended to metadata or linking to a regularly-updated separate data structure (such as a .csv, .json, or .xml) in a designated directory.

Within G-FIBMID, the DSV would incorporate instrument-specific hardware, environmental, and software condition indicators selected according to known degradation mechanisms, measurement feasibility, and validation requirements. With validated instrument-specific calibration models, DSV information could support the estimation and flagging of measurement bias before downstream analysis. Unauthorized changes to signed, externally anchored records may be detectable under an appropriately implemented attestation and tamper-evident logging design; these mechanisms alone do not establish the physical accuracy of the sensor signal (Regenscheid, 2018; Laurie, Messeri and Stradling, 2021; Birkholz et al., 2023).

Historical spaceflight heritage reinforces the relevance of this example. The Rosetta mission incorporated the Micro-Imaging Dust Analysis System (MIDAS), which used AFM to characterize cometary dust (Riedler et al., 2007). Similarly, the Phoenix Mars Lander carried an AFM within its Microscopy, Electrochemistry, and Conductivity Analyzer (Hecht et al., 2008). In both cases, mechanical drift, tip wear, calibration stability, and environmental stress could have significantly influenced interpretation. Incorporating degradation-aware digital twin architectures into future payloads would extend this heritage by ensuring that instrument evolution is explicitly modeled and securely tracked. Chen et al. (2004) document multiple-tip imaging effects, while Orji et al. (2020) provide more direct experimental evidence regarding AFM probe-tip wear; Figure 2 is an illustrative schematic and not a reproduced experimental micrograph.

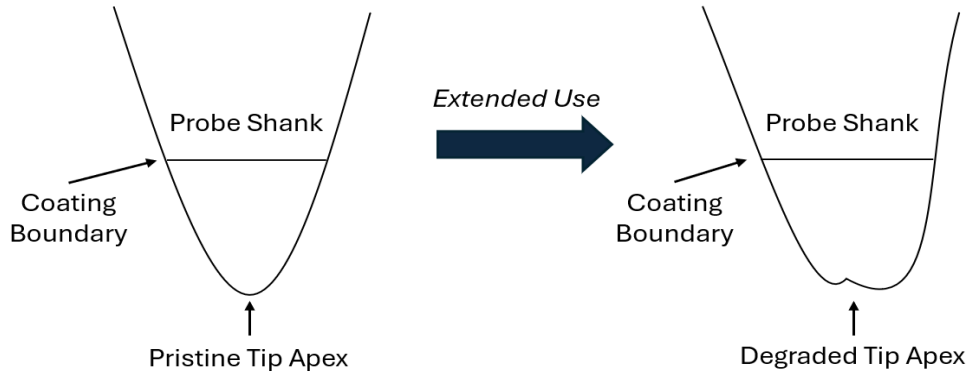

Figure inspired by Chen et al, 2004

Figure 2: Illustrative schematic of AFM tip changes during extended use. See Chen et al. (2004) for multiple-tip artifacts and Orji et al. (2020) for experimental tip-wear measurements. Not to scale

Extending the AFM example to mission deployment illustrates lifecycle continuity. An AFM integrated into an orbital or deep-space biological payload would require engineering controls for radiation-related electronic effects, thermal management and calibration; actual exposure and degradation depend on the mission environment and design (Dodd and Massengill, 2003; Haider et al., 2019). Firmware updates transmitted mid-mission could alter measurement interpretation, and actuator drift could accelerate under radiation exposure. Within G-FIBMID, onboard systems may continuously record relevant operational parameters and aggregate them into signed degradation snapshots. AFM export formats vary by instrument and software. OME provides precedents for standardized microscopy metadata and interoperable imaging formats, but the proposed G-FIBMID DSV-to-AFM metadata mapping and any JSON implementation require explicit specification (Open Microscopy Environment (OME), n.d.; Goldberg et al., 2005; Moore et al., 2021). Bias correction algorithms operating under high-latency conditions would estimate instrument-induced offsets using validated degradation history. Anomalies exceeding expected degradation trajectories would trigger prioritized telemetry review. The proposed ground-to-flight pathway would integrate terrestrially established drift models with secure autonomous monitoring, subject to mission-specific validation.

While AFM functions as a demonstrative example, the architectural design is broadly applicable to any degradation sensitive biological instrumentation: devices such as sequencers, fluorescence imagers, environmental biosensors, and lab-on-a-chip platforms are also subject to physical degradation during their use. Each specific instrument type could require a unique snapshot tailored to its internal configuration. The guiding principle is to associate each biological measurement with cryptographically authenticated records of instrument condition and acquisition context. G-FIBMID transforms hardware evolution from an unobserved liability into a structured, securable dimension of biological measurement, preserving architectural primacy while remaining instrument-agnostic.

4. Cyberbiosecurity and Mission Autonomy Implications

Scholarship on cyberbiosecurity examines the intersection of biosecurity and cybersecurity, including national and mission-oriented implications (Murch et al., 2018; George, 2019; Potter and Palmer, 2023). Convergence-oriented cybersecurity scholarship has highlighted interdisciplinary approaches (Abdo and Hossain, 2025), while cyberbiosecurity literature has addressed emerging mission-specific space concerns (Dove et al., 2025). This paper proposes extending cyberbiosecurity considerations to the integrity of biological interpretation, drawing on predictive physiological modeling as an adjacent precedent rather than claiming prior validation of a degradation-aware biological twin (Potter et al., 2024). Cyberbiosecurity research has examined risk perception, laboratory attack surfaces, data-mining approaches, and malicious-content persistence in biological workflows (Richardson et al., 2019; Millett et al., 2019; Crawford et al., 2023; Shankar et al., 2024; Pope, 2026); these are related but distinct from instrument degradation. In extreme environments, reliable biological conclusions require secure hardware state continuity. Scientific validity, operational safety, and cybersecurity thus converge to one architectural problem.

The relevance of degradation-aware provenance may extend beyond spaceflight instrumentation to connected biological sensing and healthcare settings, where measurements inform computational interpretation and security-sensitive decisions. Herbst, Bergkemper and Lipps (2023) examined gait-based biometric recognition using pressure-sensor data from instrumented footwear and described data transmission and encryption considerations. Möllenhoff et al. (2025) presented a prospective 6G-enabled smart-hospital architecture and use cases involving wireless body-area monitoring, while identifying cybersecurity, privacy and regulatory challenges. Neither study evaluates cumulative instrument degradation or validates G-FIBMID. Rather, they illustrate adjacent applications in which recording sensor configuration, operational condition and acquisition history could improve the traceability and interpretation of measured signals. Such extensions remain prospective and require application-specific validation.

Traditional cybersecurity frameworks prioritize data confidentiality, availability, and integrity. In extreme environment biology, adversarial impact can occur subtly: calibration constants, firmware versions, timestamps, or degradation logs may be altered or truncated without directly changing raw biological measurements (Potter and Palmer, 2021; Crawford et al, 2023; Dove et al, 2025). Such actions may introduce interpretive bias, motivating an authenticated chain of device-state evidence and measurement metadata (Regenscheid, 2018; Birkholz et al., 2023). Additionally, degradation of hardware may affect boot-loading, sector integrity, or other hard stops to hardware functionality. If vulnerabilities are exposed as a result of physical degradation, they offer an attack surface area to malicious actors.

G-FIBMID would associate signed DSV updates with biological measurements and an auditable event history. Properly anchored, tamper-evident logs may expose record modifications, but a suspicious residual is not proof of malicious activity (Laurie, Messeri and Stradling, 2021; Birkholz et al., 2023). As biological analysis becomes more automated, unrecognized instrumentation artifacts may be learned as biological features. The proposed architecture could document model-training inputs, degradation alerts and correction actions; whether this reduces analytical bias remains an empirical question.

During deep-space missions, communication delays may prevent immediate ground oversight. G-FIBMID therefore proposes onboard monitoring that records authenticated degradation-state snapshots, detects deviations from expected behavior, and supports operational decision-making. Any autonomous adjustment of acquisition parameters or suspension of measurements would be governed by predefined, mission-specific operating limits, validated decision rules, and fail-safe procedures rather than unconstrained machine-learning outputs. Where instrument-specific calibration models have been validated, degradation histories could inform bias estimation, while correction actions and operational decisions would be time-stamped and cryptographically logged for subsequent ground review. Defining, testing, and verifying these decision thresholds and safety mechanisms remains an essential objective for future research.

Radiation-induced memory corruption adds complexity. In high-radiation environments, stochastic bit flips may resemble adversarial manipulation. This challenge necessitates the use of radiation-hardened computer systems, which employ techniques like error-correcting codes, redundancy, and specialized shielding to mitigate the effects of ionizing radiation. Delta-DSV comparisons may support anomaly detection by contrasting observed and expected state trajectories, but they cannot independently attribute an anomaly to radiation, accidental error or malicious tampering (Dodd and Massengill, 2003; Birkholz et al., 2023). This distinction is crucial for trusting both hardware reliability and cyberbiosecurity safeguards. While motivated by spaceflight, these principles apply to terrestrial high-risk biological environments (Crawford et al, 2023; Dove et al, 2025).

High-containment laboratories, biodefense platforms, pandemic facilities, and remote monitoring all use instrumentation subject to degradation under stress. In these settings, degradation-aware digital twins may support reproducibility, transparency and investigation of interpretive manipulation, subject to validation. By integrating degradation modeling into cyberbiosecurity, G-FIBMID strengthens trustworthy biological experimentation where both biology and instrumentation evolve under stress.

5. Conclusion and Research Agenda

G-FIBMID proposes linking biological observations to authenticated, time-indexed instrument-degradation states and a predictive digital twin. This integration could improve review of measurement uncertainty without presuming that provenance proves accuracy. Core research priorities are to define DSV components and uncertainty; establish secure timestamps and trust assumptions; benchmark state predictions and correction methods against conventional calibration; and test onboard resource demands, anomaly handling and failure modes. Spaceflight AFM offers an illustrative validation scenario, while connected healthcare and high-

containment facilities provide potential extensions. Empirical studies must determine whether the architecture improves biological interpretation, auditability and mission resilience.

Ethics Declaration: An ethics declaration is not applicable to this work.

AI Declaration: AI tools within Chat-GPT, Grammarly and Google Docs were used for re-organizing the paper, including grammar, figure checks, and spelling checks.

References

Abdo, J.B. and Hossain, L. (2025) 'Interdisciplinarity of cybersecurity: Towards convergence science', Authorea Preprints. Available at: https://doi.org/10.22541/au.175372207.76327770/v1

Birkholz, H., Thaler, D., Richardson, M., Smith, N. and Pan, W. (2023) Remote ATtestation procedureS (RATS) Architecture. RFC 9334. Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC9334

Chen, Y. (2012) 'Elucidation and identification of double-tip effects in atomic force microscopy studies of biological structures', Journal of Surface Engineered Materials and Advanced Technology, 2(3), pp. 238–247. Available at: https://doi.org/10.4236/jsemat.2012.223037

Chen, Y., Cai, J., Liu, M., Zeng, G., Feng, Q. and Chen, Z. (2004) 'Research on double-probe, double- and triple-tip effects during atomic force microscopy scanning', Scanning, 26(4), pp. 155–161. Available at: https://doi.org/10.1002/sca.4950260402

Chen, Z., Luo, J., Doudevski, I., Erten, S. and Kim, S.H. (2019) 'Atomic force microscopy (AFM) analysis of an object larger and sharper than the AFM tip', Microscopy and Microanalysis, 25(5), pp. 1106–1111. Available at: https://doi.org/10.1017/S1431927619014697

Crawford, E., Bobrow, A., Sun, L., Joshi, S., Vijayan, V., Blacksell, S., Venugopalan, G. and Tensmeyer, N. (2023) 'Cyberbiosecurity in high-containment laboratories', Frontiers in Bioengineering and Biotechnology, 11, article 1240281. Available at: https://doi.org/10.3389/fbioe.2023.1240281

Dickbreder, T., Sabath, F., Höltkemeier, L., Bechstein, R. and Kühnle, A. (2023) 'unDrift: A versatile software for fast offline SPM image drift correction', Beilstein Journal of Nanotechnology, 14, pp. 1225–1237. Available at: https://doi.org/10.3762/bjnano.14.101

Dodd, P.E. and Massengill, L.W. (2003) 'Basic mechanisms and modeling of single-event upset in digital microelectronics', IEEE Transactions on Nuclear Science, 50(3), pp. 583–602. Available at: https://doi.org/10.1109/TNS.2003.813129

Dove, D., Chamberland, K., Karathanasis, S.F., Potter, L. and Palmer, X.-L. (2025) 'Integrating ethical, legal, and technological safeguards in space-focused cyberbiosecurity: AI, cloud, and crew considerations', Proceedings of the 6th International Conference on AI Research, 6(1), pp. 687–695. Available at: https://doi.org/10.34190/icair.5.1.4391

Eaton, P. and West, P. (2010) 'AFM image artefacts', in Atomic Force Microscopy. Oxford: Oxford University Press, pp. 121–138. Available at: https://doi.org/10.1093/acprof:oso/9780199570454.003.0006

Erickson, B.W., Coquoz, S., Adams, J.D., Burns, D.J. and Fantner, G.E. (2012) 'Large-scale analysis of high-speed atomic force microscopy data sets using adaptive image processing', Beilstein Journal of Nanotechnology, 3, pp. 747–758. Available at: https://doi.org/10.3762/bjnano.3.84

George, A.M. (2019) 'The national security implications of cyberbiosecurity', Frontiers in Bioengineering and Biotechnology, 7, article 51. Available at: https://doi.org/10.3389/fbioe.2019.00051

Goldberg, I.G., Allan, C., Burel, J.-M., Creager, D., Falconi, A., Hochheiser, H., Johnston, J., Mellen, J., Sorger, P.K. and Swedlow, J.R. (2005) 'The Open Microscopy Environment (OME) Data Model and XML file: open tools for informatics and quantitative analysis in biological imaging', Genome Biology, 6(5), article R47. Available at: https://doi.org/10.1186/gb-2005-6-5-r47

Gołek, F., Mazur, P., Ryszka, Z. and Zuber, S. (2014) 'AFM image artifacts', Applied Surface Science, 304, pp. 11–19. Available at: https://doi.org/10.1016/j.apsusc.2014.01.149

Haider, M.F., Giurgiutiu, V., Lin, B., Yu, L., Lam, P.-S. and Verst, C. (2019) 'Effects of gamma radiation on resonant and antiresonant characteristics of piezoelectric wafer active sensors', Journal of Nondestructive Evaluation, Diagnostics and Prognostics of Engineering Systems, 2(1), article 011001. Available at: https://doi.org/10.1115/1.4041068

Hecht, M.H. et al. (2008) 'Microscopy capabilities of the Microscopy, Electrochemistry, and Conductivity Analyzer', Journal of Geophysical Research: Planets, 113(E3), article E00A22. Available at: https://doi.org/10.1029/2008JE003077

Herbst, J., Bergkemper, L. and Lipps, C. (2023) 'Step by step: A gait-centric approach to footbed-based recognition' [preprint]. Available at: https://doi.org/10.13140/RG.2.2.20711.87208

Hörz, M. (2021) HxD Hex Editor (Version 2.5.0.0) [Computer software]. Available at: https://mh-nexus.de/en/hxd/

Hu, Z., Bhattacharya, S. and Butte, A.J. (2022) 'Application of machine learning for cytometry data', Frontiers in Immunology, 12, article 787574. Available at: https://doi.org/10.3389/fimmu.2021.787574

International Organization for Standardization (ISO) (2025) ISO 13381-1:2025: Condition monitoring and diagnostics of machine systems — Prognostics — Part 1: General guidelines and requirements. Geneva: ISO. Available at: https://www.iso.org/standard/88029.html

Klapetek, P., Nečas, D., Campbellová, A., Yacoot, A. and Koenders, L. (2011) 'Methods for determining and processing 3D errors and uncertainties for AFM data analysis', Measurement Science and Technology, 22(2), article 025501. Available at: https://doi.org/10.1088/0957-0233/22/2/025501

Klapetek, P., Nečas, D., Heaps, E., Sauvet, B., Klapetek, V., Valtr, M., Korpelainen, V. and Yacoot, A. (2024) 'Stitching accuracy in large area scanning probe microscopy', Measurement Science and Technology, 35(12), article 125026. Available at: https://doi.org/10.1088/1361-6501/ad7a13

Laurie, B., Messeri, E. and Stradling, R. (2021) Certificate Transparency Version 2.0. RFC 9162. Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC9162

Märtens, K., Bortolomeazzi, M., Montorsi, L., Spencer, J., Ciccarelli, F. and Yau, C. (2023) 'Rarity: discovering rare cell populations from single-cell imaging data', Bioinformatics, 39(12), article btad750. Available at: https://doi.org/10.1093/bioinformatics/btad750

Millett, K., dos Santos, E. and Millett, P.D. (2019) 'Cyber-biosecurity risk perceptions in the biotech sector', Frontiers in Bioengineering and Biotechnology, 7, article 136. Available at: https://doi.org/10.3389/fbioe.2019.00136

Möllenhoff, C., Agarwal, B., Herbst, J., Rüb, M., Petzold, T., Pabst, T., Irmer, R., Lipps, C., Schotten, H.D., Neumuth, T. and Rockstroh, M. (2025) 'Towards 6G-connected healthcare: Perspectives, risks and real-world applications for smart hospitals', Proceedings of the 2025 47th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 1–7. Available at: https://doi.org/10.1109/EMBC58623.2025.11253874

Moore, J., Allan, C., Besson, S., Burel, J.-M., Diel, E., Gault, D., Kozlowski, K., Lindner, D., Linkert, M., Manz, T., Moore, W., Pape, C., Tischer, C. and Swedlow, J.R. (2021) 'OME-NGFF: a next-generation file format for expanding bioimaging data-access strategies', Nature Methods, 18, pp. 1496–1498. Available at: https://doi.org/10.1038/s41592-021-01326-w

Murch, R.S., So, W.K., Buchholz, W.G., Raman, S. and Peccoud, J. (2018) 'Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy', Frontiers in Bioengineering and Biotechnology, 6, article 39. Available at: https://doi.org/10.3389/fbioe.2018.00039

Nečas, D. and Klapetek, P. (2017) 'Study of user influence in routine SPM data processing', Measurement Science and Technology, 28(3), article 034014. Available at: https://doi.org/10.1088/1361-6501/28/3/034014

Open Microscopy Environment (OME) (n.d.) Bio-Formats. Available at: https://www.openmicroscopy.org/bio-formats/

Orji, N.G., Dixson, R.G., Lopez, E. and Irmer, B. (2020) 'Wear comparison of critical dimension-atomic force microscopy tips', Journal of Micro/Nanolithography, MEMS, and MOEMS, 19(1), article 014004. Available at: https://doi.org/10.1117/1.JMM.19.1.014004

Petrov, M., Canena, D., Kulachenkov, N., Kumar, N., Nickmilder, P., Leclère, P. and Sokolov, I. (2024) 'Mechanical spectroscopy of materials using atomic force microscopy (AFM-MS)', Materials Today, 80, pp. 218–225. Available at: https://doi.org/10.1016/j.mattod.2024.08.021

Pope, T. (2026) 'Sleeper code in protein data files as cyber adversarial vectors', Proceedings of the 21st International Conference on Cyber Warfare and Security, 21(1), pp. 624–632. Available at: https://doi.org/10.34190/iccws.21.1.4459

Potter, L. and Palmer, X.-L. (2021) 'Human factors in biocybersecurity wargames', in Arai, K. (ed.) Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1. Cham: Springer, pp. 666–673. Available at: https://doi.org/10.1007/978-3-030-73100-7_48

Potter, L. and Palmer, X.-L. (2023) 'Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination', in Greenbaum, D. (ed.) Cyberbiosecurity: A New Field to Deal with Emerging Threats. Cham: Springer, pp. 37–69. Available at: https://doi.org/10.1007/978-3-031-26034-6_4

Potter, L., Shetty, S., Karahan, S. and Palmer, X.-L. (2024) 'Biocybersecurity and applications of predictive physiological modelling', International Journal of System of Systems Engineering, 14(4), pp. 349–361. Available at: https://doi.org/10.1504/IJSSE.2024.139410

Regenscheid, A.R. (2018) Platform Firmware Resiliency Guidelines. NIST Special Publication 800-193. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-193

Richardson, L.C., Connell, N.D., Lewis, S.M., Pauwels, E. and Murch, R.S. (2019) 'Cyberbiosecurity: A call for cooperation in a new threat landscape', Frontiers in Bioengineering and Biotechnology, 7, article 99. Available at: https://doi.org/10.3389/fbioe.2019.00099

Riedler, W. et al. (2007) 'MIDAS – The Micro-Imaging Dust Analysis System for the Rosetta Mission', Space Science Reviews, 128(1–4), pp. 869–904. Available at: https://doi.org/10.1007/s11214-006-9040-y

Rosenthal, D.S.H. (2010) 'Keeping bits safe: How hard can it be?', Communications of the ACM, 53(11), pp. 47–55. Available at: https://doi.org/10.1145/1839676.1839692

Sadewasser, S., Nicoara, N. and Solares, S.D. (2018) 'Artifacts in time-resolved Kelvin probe force microscopy', Beilstein Journal of Nanotechnology, 9, pp. 1272–1281. Available at: https://doi.org/10.3762/bjnano.9.119

Sansone, S.-A. et al. (2012) 'Toward interoperable bioscience data', Nature Genetics, 44(2), pp. 121–126. Available at: https://doi.org/10.1038/ng.1054

Shankar, D.D., Azhakath, A.S., Khalil, N., Sajeev, J., Mahalakshmi, T. and Sheeba, K. (2024) 'Data mining for cyber biosecurity risk management – A comprehensive review', Computers & Security, 137, article 103627. Available at: https://doi.org/10.1016/j.cose.2023.103627

Sokolov, I. (2024) 'On machine learning analysis of atomic force microscopy images for image classification, sample surface recognition', Physical Chemistry Chemical Physics, 26(15), pp. 11263–11270. Available at: https://doi.org/10.1039/D3CP05673B

Sullan, R.M.A., Churnside, A.B., Nguyen, D.M., Bull, M.S. and Perkins, T.T. (2013) 'Atomic force microscopy with sub-picoNewton force stability for biological applications', Methods, 60(2), pp. 131–141. Available at: https://doi.org/10.1016/j.ymeth.2013.03.029

Tao, F., Zhang, H., Liu, A. and Nee, A.Y.C. (2019) 'Digital twin in industry: State-of-the-art', IEEE Transactions on Industrial Informatics, 15(4), pp. 2405–2415. Available at: https://doi.org/10.1109/TII.2018.2873186

Voigtländer, B. (2019) Atomic Force Microscopy. 2nd edn. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-13654-3

Wikimedia Commons (n.d.) 'Mona Lisa.jpg' [Digital image; source: Musée du Louvre; original artwork by Leonardo da Vinci]. Available at: https://commons.wikimedia.org/wiki/File:Mona_Lisa.jpg

World Wide Web Consortium (W3C) (2013) PROV-O: The PROV Ontology. W3C Recommendation, 30 April. Edited by T. Lebo, S. Sahoo and D. McGuinness. Available at: https://www.w3.org/TR/prov-o/

Appendix: Supplementary Figure A: Glossary of terms used in this work

Glossary	
Autonomous Biological Systems	Biological measurement platforms designed to acquire or process data with limited real-time human oversight. Mission autonomy is a proposed G-FIBMID use case, not a demonstrated capability (Dove et al., 2025; Potter and Palmer, 2023).
Cryptographic Provenance	Documentation of data origin and transformations, reinforced by attestation and tamper-evident records. It supports record integrity but does not establish physical measurement accuracy (W3C, 2013; Birkholz et al., 2023; Laurie, Messeri and Stradling, 2021).
Degradation State Vector (DSV)	A G-FIBMID-defined, time-indexed set of instrument-condition indicators, such as exposure, wear, drift and configuration. The proposed representation draws on equipment prognostics and digital-twin methods (ISO, 2025; Tao et al., 2019).
Digital Twin	A computational representation of a physical system that incorporates operating data to characterize or predict system behavior. In G-FIBMID, a twin would estimate an instrument's expected degradation trajectory (Tao et al., 2019).
Hardware Root of Trust	A hardware-anchored security foundation supporting protected key operations, firmware-integrity checks and evidence for device-state attestation; it cannot certify the correctness of sensor measurements (Regenscheid, 2018; Birkholz et al., 2023).
Instrument Bias Correction	Estimation and, when validated calibration permits, adjustment of systematic measurement error. AFM drift-correction methods exist, but DSV-guided correction in G-FIBMID remains proposed (Klapetek et al., 2011; Dickbreder et al., 2023).
Machine Learning Integrity	Within G-FIBMID, traceable, quality-controlled measurement inputs for computational analysis, intended to limit interpretation of instrument artifacts as biological patterns. This safeguard is proposed for imaging analytics (Hu, Bhattacharya and Butte, 2022; Märtens et al., 2023).
Mission-Phase Modeling	Accounting for changing stresses and monitoring requirements across pre-flight, launch, flight and deep-space operations. This mission-specific approach is proposed by G-FIBMID; the cited work provides space-cyberbiosecurity context (Dove et al., 2025).
Radiation-Induced Drift	Gradual changes in the performance of radiation-sensitive components under accumulated exposure, distinguished from discrete single-event upsets in microelectronics (Haider et al., 2019; Dodd and Massengill, 2003).
Secure Data Lineage	A traceable record of how data were acquired, transformed and associated with instrument-state evidence, using provenance descriptions and applicable security attestations (W3C, 2013; Birkholz et al., 2023).
Space Biology	The study of biological processes and systems in spaceflight or simulated-space conditions, including altered gravity and radiation exposure. The cited work provides related mission context, not a formal definition (Dove et al., 2025).
Tamper-Evident Logging	Logging designed to make certain changes to recorded entries detectable through cryptographic linkage and verification. Append-only transparency logs provide one relevant technical model (Laurie, Messeri and Stradling, 2021).
Biometric Sensing and Authentication	Use of physiological or behavioral signals, such as gait, for identity recognition or verification. Sensor provenance may affect the interpretation of these signals (Herbst, Bergkemper and Lipps, 2023).
Connected Healthcare Cyber-Physical Systems	Interconnected sensing, computation and communication technologies supporting healthcare monitoring and workflows, with associated security and privacy challenges; a possible G-FIBMID application (Möllenhoff et al., 2025).

Source note: ISO 13381-1:2025 supports general equipment prognostics; it does not define or validate the G-FIBMID DSV. Citations to related applications supply context, not proof of G-FIBMID performance.