WHITE PAPER

Analog Guard® Mixed-Signal Physical-Layer Encryption and DARK

The Distributed Analog Reconstruction-Key System

This white paper presents DARK as a reconstruction-centric security architecture built on Analog Guard® mixed-signal physical-layer encryption. It reframes security from possession of a recoverable key toward governed establishment, validation, and collapse of reconstruction conditions.

Document Type	Technical White Paper
Prepared By	Chris M. Hymel, Ph.D.
Organization	Analog Guard, Inc.
Version	White Paper Format Draft
Date	June 2026
Intended Audience	Technical reviewers, investors, cybersecurity architects, and strategic partners

Core thesis: Analog Guard® and DARK shift the protected asset from a stored secret to the governed ability to create transient reconstruction conditions inside hardware-bound, synchronization-governed replay environments.

Contents

Document Orientation

Element	White Paper Function
Executive summary	States the thesis and summarizes DARK in business and technical terms.
Problem context	Distinguishes DARK from key-centric cryptography, threshold schemes, HSMs, PUFs, and replay rejection.
Technical foundation	Explains Analog Guard® carrier, temporal, waveform, and analog-state mechanisms.
Architecture	Defines DARK replay domains, synchronization governance, replay compatibility, and hardware-bound invalidation.
Implementation models	Shows representative FPGA/DAC, multi-node, mixed-signal, SDR, and optical embodiments.
Strategic implications	Frames why reconstructability governance complements strong cryptography and post-quantum security.

Use and Validation Note

This document is provided for technical discussion and strategic evaluation. It is not a product specification, security certification, legal opinion, investment solicitation, or guarantee of resistance to any particular attack method. Implementation-specific conclusions require independent engineering validation, threat modeling, and review by qualified advisors.

1. Executive Summary

Modern cybersecurity architectures are commonly organized around recoverable objects: encryption keys, credentials, certificates, tokens, secrets, shares, device responses, or authorization artifacts. Conventional systems may protect those objects, divide them among custodians, reconstruct them inside protected hardware, derive them from device responses, erase them after use, or reject replayed transactions. The Distributed Analog Reconstruction-Key System (DARK) reflects a different architectural premise.

DARK builds upon the Analog Guard® mixed-signal physical-layer encryption framework, in which dynamically evolving analog conditions participate directly in the protection and reconstruction of information-bearing signals. Rather than treating the communication signal as a passive carrier of encrypted data, Analog Guard® uses physical signal behavior, carrier relationships, temporal modulation, waveform evolution, and analog-state dependencies as part of the reconstruction environment.

DARK extends that foundation into a synchronization-governed replay coordination architecture. Reconstruction capability is not treated as a stored object to be retrieved or recombined. Authorized reconstruction emerges only when operationally incomplete replay-domain participation components satisfy replay-coordination criteria within replay-isolated reconstruction hardware during a bounded replay interval.

A replay domain may contribute a waveform condition, timing condition, synchronization relationship, routing state, transport relationship, authorization state, validation condition, or governance condition. Individually, these components remain incomplete. Collectively, and only during synchronized participation, they may establish transient replay compatibility sufficient to support reconstruction.

The architecture evaluates replay compatibility using measurable replay-state indicators, including timing deviation, replay jitter, phase deviation, waveform correlation, waveform coherence, spectral divergence, replay-buffer state, replay-routing state, synchronization-reference state, transport-state condition, authorization-state condition, and related coherence indicators. Replay-governance circuitry may compare these indicators against fixed, adaptive, policy-controlled, statistically derived, hardware-controlled, or dynamically updated thresholds.

When replay-coordination criteria are satisfied, reconstruction capability may be transiently enabled. When synchronization continuity is lost, authorization fails, replay perturbation occurs, replay-state indicators diverge, or reconstruction criteria are no longer satisfied, the system may physically modify replay pathways, replay buffers, synchronization references, routing-fabric configurations, timing relationships, waveform-conditioning parameters, replay-domain isolation states, or authorization-control states.

Those physical modifications may induce replay incompatibility propagation, entropy divergence, replay-state orphaning, topology mutation, replay collapse, or other anti-stabilization behavior. The objective is not merely to erase a key after use. The objective is to prevent stable replay compatibility from persisting or reforming outside authorized synchronized replay participation.

Representative DARK implementation architectures include FPGA/DAC deterministic-latency replay, multi-node quorum-governed reconstruction, analog or mixed-signal waveform conditioning, and software-defined radio/optical transport replay. These examples demonstrate how the broader architecture may be realized using programmable logic, deterministic-latency DAC release, distributed node governance, physical waveform-conditioning relationships, carrier/phase/timing relationships, wavelength-separated replay pathways, optical-path isolation, and replay-governed transport reassignment.

Viewed broadly, Analog Guard® and DARK describe a transition from key-centric security toward reconstruction-centric security. The protected capability is no longer limited to possession of a stored secret. It becomes the governed ability to establish, validate, maintain, and then collapse the conditions under which reconstruction can occur.

Key Takeaways

Theme	Takeaway
Security model	The architecture is reconstruction-centric rather than solely key-centric.
Protected asset	The protected asset is the governed ability to establish reconstruction conditions.
DARK mechanism	Authorized reconstruction emerges only during synchronized replay-domain participation within bounded hardware conditions.
Invalidation model	Failure of authorization, synchronization, coherence, or replay coordination may physically modify replay conditions and collapse compatibility.
Strategic role	DARK complements cryptographic algorithms by controlling the physical, temporal, and governance conditions under which information becomes recoverable.

2. Purpose, Audience, and Scope

This white paper explains the technical and architectural rationale for DARK, the Distributed Analog Reconstruction-Key System, as an extension of Analog Guard® mixed-signal physical-layer encryption.

The intended audience includes technical reviewers, cybersecurity architects, defense and critical-infrastructure stakeholders, investors, strategic partners, and patent or diligence reviewers evaluating the difference between conventional key protection and reconstruction-governed security.

The scope is architectural. The paper describes representative mechanisms, evaluation criteria, and implementation embodiments. It does not assert immunity from future analytical methods, quantum computing, artificial intelligence, insider compromise, or all implementation-level attacks.

Terminology Used in This Paper

Term	Use in this white paper
Analog Guard®	The mixed-signal physical-layer encryption framework that uses physical signal behavior as part of the protection and recovery environment.
DARK	The distributed architecture that governs synchronized replay-domain participation and reconstruction-key conditions.
Reconstruction-key	A distributed recovery capability formed by coordinated analog-state, replay-domain, synchronization, validation, and governance conditions.
Replay domain	A separately maintained operational condition that contributes to synchronized reconstruction.

3. Security Context and Architectural Problem

Introduction

Modern cybersecurity was built upon a durable assumption: information can be protected mathematically. Encryption systems transform readable information into forms that are difficult to interpret without possession of a corresponding cryptographic key. Whether protecting military communications, financial transactions, industrial control systems, cloud infrastructure, or consumer devices, the dominant security paradigm has generally remained key-centric.

That approach has proven extraordinarily successful. However, it also shares a common architectural characteristic. In most conventional systems, the communication channel serves primarily as a transport mechanism. Encryption

protects the information being transmitted, while the underlying signal environment remains secondary to the security model itself.

Analog Guard® proposes a different perspective. Rather than treating the communication signal as a passive carrier of encrypted information, Analog Guard® incorporates the physical behavior of the signal into the protection architecture. U.S. Patent Nos. 12,126,720 and 12,615,149 describe dynamic analog processes that alter carrier behavior, timing relationships, modulation characteristics, waveform structure, resonant interactions, and spectral content during transmission and recovery.

In this architecture, security emerges not solely from computational complexity, but from coordinated interaction of physical signal processes that participate directly in the creation, transport, and reconstruction of protected information.

This distinction matters because modern interception systems increasingly rely upon stable signal characteristics. Signal-intelligence platforms, electronic-surveillance systems, and machine-learning-based analytical tools attempt to identify recurring behaviors within communications environments. Carrier frequencies, spectral signatures, timing periodicity, modulation structures, synchronization patterns, pulse intervals, and transmission characteristics can reveal operational information even when encrypted data remains inaccessible.

Analog Guard® is designed to reduce reliance on stable reference points. It introduces evolving analog-state conditions through mechanisms such as dynamic carrier generation, analog key modulation, Phase-Linked Temporal Nonlinear Modulation (PLTNM), orthogonal signal pathways, multi-band processing environments, and resonant analog transformations. Rather than maintaining a fixed transmission structure, the signal environment itself becomes an active participant in protection and recovery.

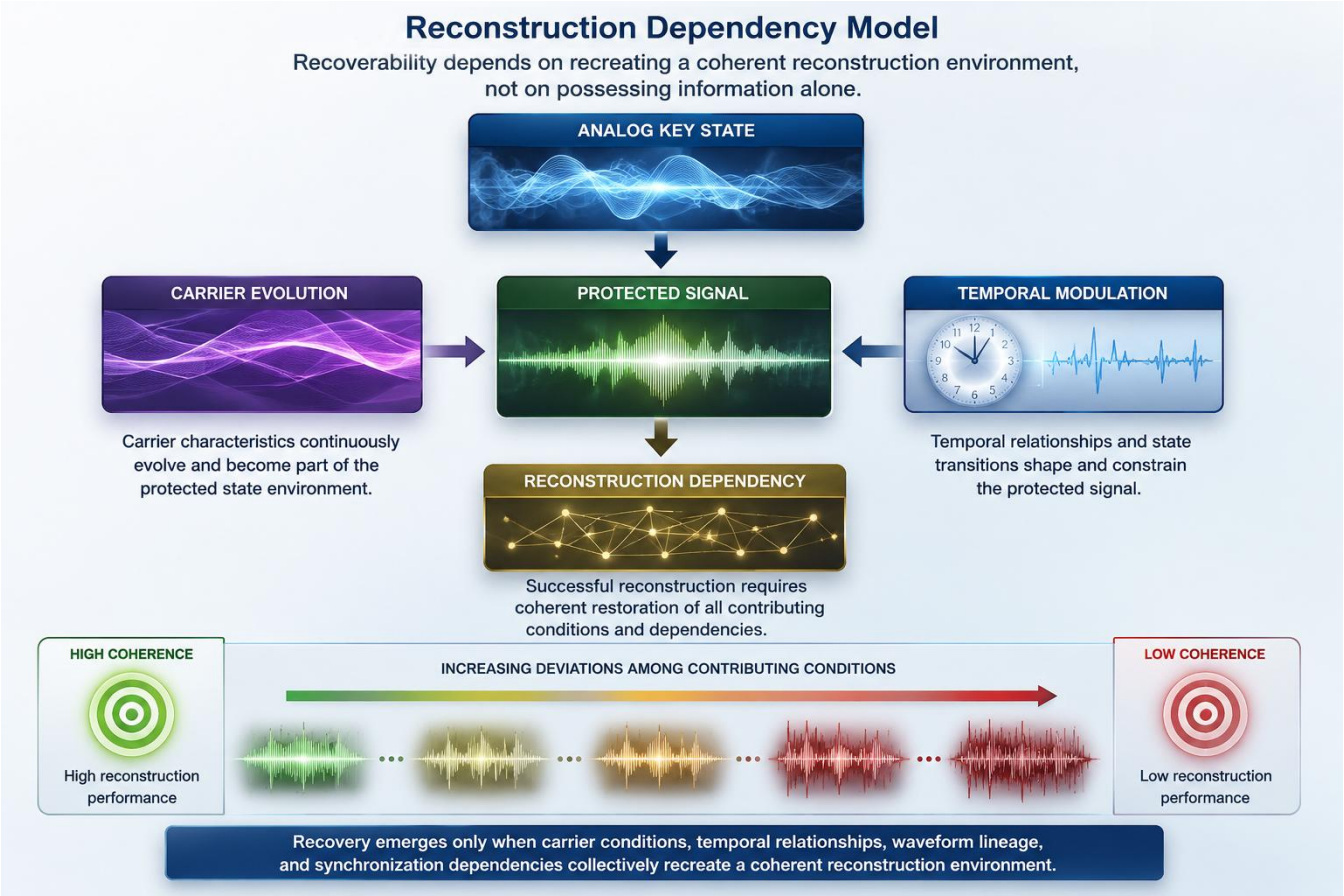

Figure 1 *conceptually illustrates this principle. The figure shows reconstruction capability emerging when carrier conditions, temporal relationships, waveform lineage, and synchronization dependencies remain sufficiently coherent. As those conditions diverge, reconstruction performance degrades, emphasizing that recoverability depends upon environmental coherence rather than possession of information alone.*

As a result, successful recovery requires more than possession of information alone. Recovery depends upon recreating an appropriate analog environment, including carrier relationships, timing structures, modulation conditions, waveform dependencies, resonant behaviors, and synchronization relationships that participated in the original encryption and analog key reconstruction process.

Conventional Systems Distinguished

Conventional cryptographic and secure-communication systems generally assume that some recoverable object exists and must be protected. That object may be a key, key share, credential, certificate, token, secret, hardware-protected value, device response, or authorization artifact. The system may store it, divide it, encrypt it, reconstruct it, validate access to it, or erase it after use. In each case, the security model remains organized around something that can be possessed, recovered, reassembled, derived, or authorized.

Threshold-cryptography systems divide a secret into shares and permit reconstruction when a sufficient number of shares are combined. Distributed key-management systems coordinate custody of key material or access rights across multiple domains. Hardware security modules and secure enclaves protect keys or sensitive operations within controlled hardware boundaries. Physically unclonable functions derive responses from device-specific physical variation. Replay-attack prevention systems reject stale or repeated transactions. Synchronization-based communication systems coordinate timing, phase, or carrier behavior. Zeroization systems erase stored secrets or key material.

DARK is framed differently. Reconstruction capability does not depend on retrieval, recombination, possession, release, or erasure of a singular stored key or key share. It emerges only when distributed replay-domain participation components satisfy synchronization-conditioned replay-compatibility criteria within replay-isolated reconstruction hardware during a bounded replay interval.

This distinction is central. DARK does not merely place a key inside a more secure container, divide a key among more custodians, or erase a key more aggressively after use. It makes replay compatibility itself the governed reconstruction condition. The system may then physically invalidate that compatibility by modifying timing relationships, synchronization references, replay buffers, replay pathways, routing configurations, waveform-conditioning parameters, authorization states, or transport relationships.

The result is a reconstruction model in which authorized operation depends on transient synchronized replay participation, while anti-stabilization behavior, incompatibility propagation, entropy divergence, replay-state orphaning, topology mutation, and replay collapse inhibit persistent replay compatibility outside the authorized operating interval.

4. Analog Guard Technical Foundation

Dynamic Carrier Environments

Traditional communication systems generally treat the carrier as a transport mechanism whose purpose is to convey information from one location to another. Although modern systems may employ frequency hopping, spread-spectrum techniques, adaptive modulation, or other signal-management methods, the carrier typically remains subordinate to the information being transmitted. Encryption protects the message, while the carrier functions primarily as the delivery medium.

Even when encrypted information cannot be directly recovered, the carrier can reveal operational information. Carrier frequency, bandwidth, spectral occupancy, modulation behavior, temporal characteristics, power distribution, synchronization structures, and transmission stability can assist classification, link identification, and behavioral profiling.

Analog Guard® changes the role of the carrier. Rather than relying on a relatively stable carrier environment, the architecture permits carrier behavior to evolve as part of the protection process. The carrier becomes an active participant in the protected analog-state environment rather than a passive transport layer.

When carrier behavior participates in formation of the protected signal environment, successful recovery increasingly depends upon reproducing the relevant carrier conditions. Frequency behavior, modulation interactions, phase relationships, spectral evolution, timing dependencies, and analog transformations become part of the reconstruction context.

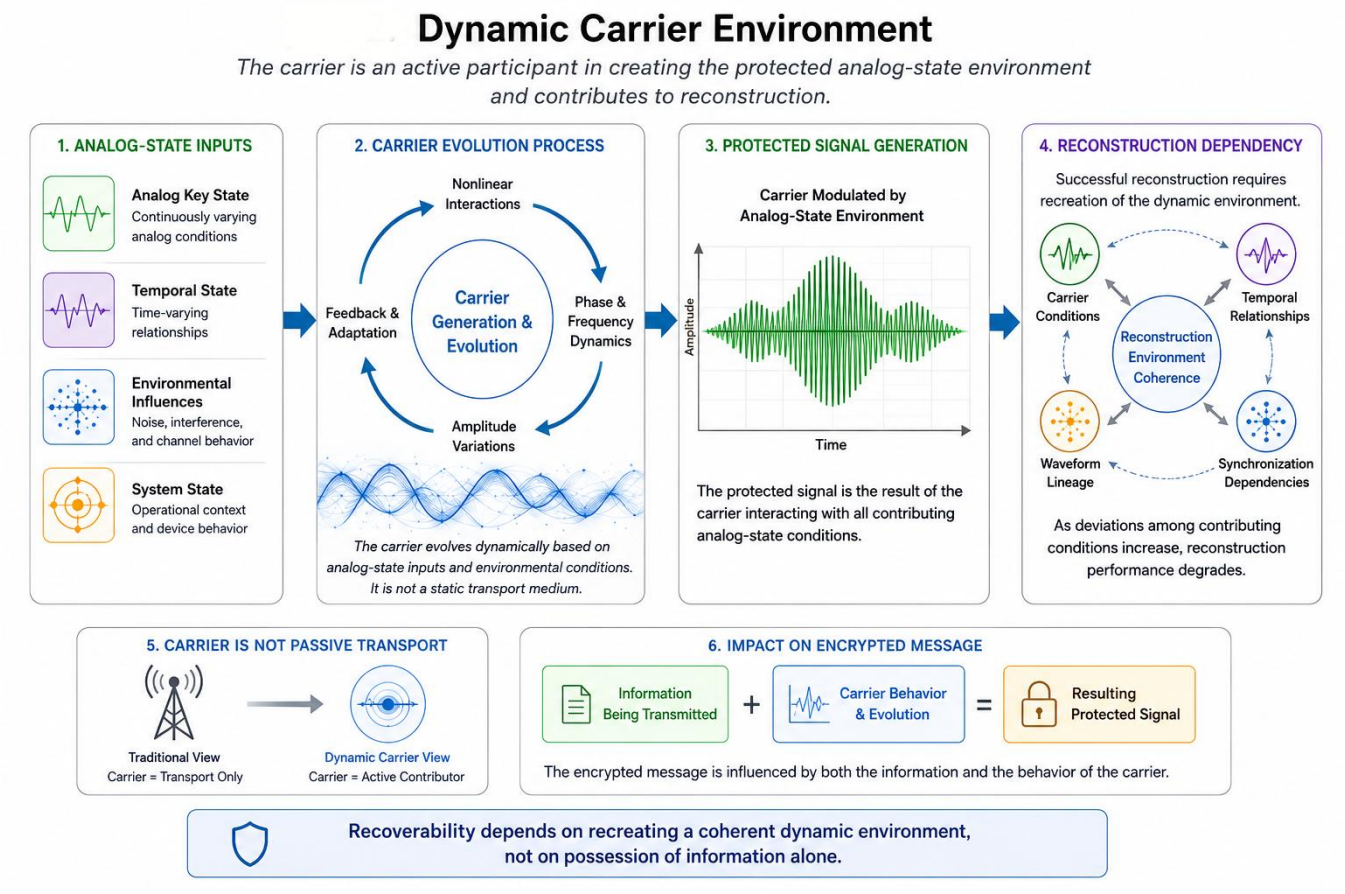

Figure 2 *(Dynamic Carrier Environment) conceptually illustrates carrier evolution as an active contributor to the protected analog-state environment rather than merely a transport mechanism.*

This is the first transition from signal transport to reconstruction dependency. The carrier continues to support communication, but it also helps create the analog-state conditions required for authorized recovery. As system complexity increases, these carrier-dependent relationships may be combined with temporal modulation, parallel signal pathways, orthogonal processing structures, and additional analog transformation domains.

Parallel Signal Paths And Analog-State Partitioning

Analog Guard® also uses multiple simultaneous signal pathways operating within a coordinated protection environment. In conventional communications systems, parallel channels often increase throughput, improve reliability, provide redundancy, or enhance bandwidth utilization. In Analog Guard®, parallel pathways can also contribute to formation of the protected signal environment itself.

This introduces analog-state partitioning. Instead of concentrating all relevant signal characteristics within a single transmission domain, portions of the operating state may exist across several independently evolving signal environments. One pathway may contribute carrier behavior, another may contribute temporal structure, another may contribute transformation history, and another may contribute waveform-conditioning behavior.

This distribution is not merely signal routing. Each pathway can develop local state characteristics while participating in a broader system-level operating condition. Observation of one pathway may reveal meaningful local behavior, but that observation does not necessarily reveal the broader context in which the pathway participates.

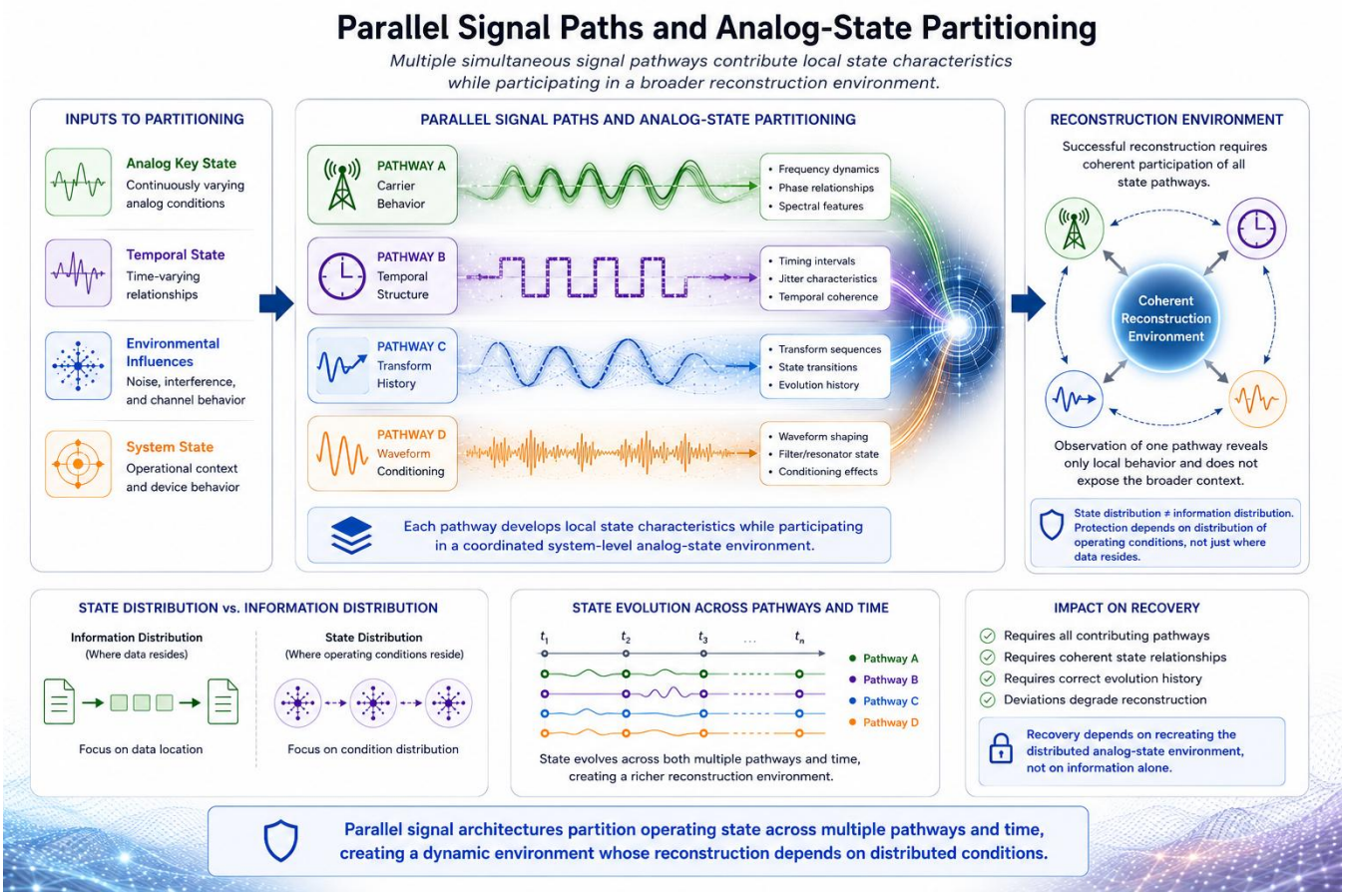

Figure 3 *illustrates multiple pathways contributing local state characteristics while participating in a broader reconstruction environment.*

State distribution differs from information distribution. Information distribution concerns where data resides. State distribution concerns where operating conditions reside. DARK and Analog Guard® increasingly rely on the latter: the protected environment is defined by the distribution of conditions that influence how information exists, evolves, and may be recovered.

Viewed in this way, parallel signal architectures become mechanisms for partitioning operational state. Once state can be partitioned across multiple pathways, it can also evolve across time, creating a richer reconstruction environment whose behavior reflects both distribution and continuity.

PLTNM And Temporal State Architecture

Phase-Linked Temporal Nonlinear Modulation (PLTNM) introduces controlled temporal transformations into the protected signal environment. Rather than preserving a fixed temporal structure throughout transmission and recovery, PLTNM allows temporal relationships to participate directly in the evolution of system state.

In practical terms, signal components may be reordered, temporal offsets may vary, processing sequences may change, and timing relationships may adapt dynamically. These behaviors are not merely signal manipulations. They contribute to the operating state of the protected environment.

This distinction introduces temporal state architecture: the collection of relationships that define how operating conditions evolve through time. Conventional timing structures coordinate transmission and reception. Temporal state architecture influences how the protected environment develops, how state transitions occur, and how successive operating conditions relate to one another.

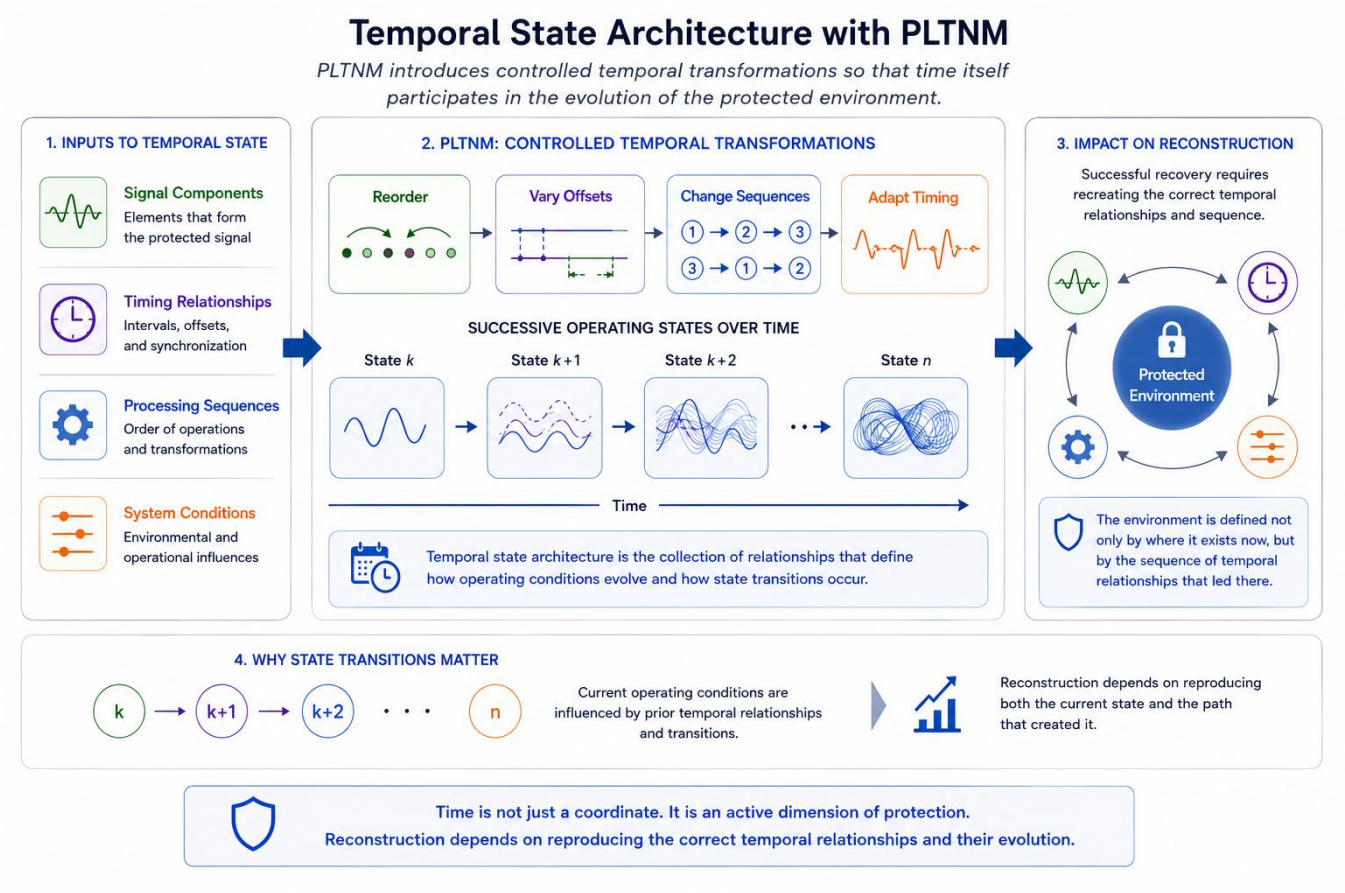

Figure 4 *illustrates successive operating states evolving through controlled temporal transitions.*

A static operating state can often be described from a single observation. A temporal operating state cannot. Understanding it requires understanding the sequence of relationships through which that state evolved. In this sense, the system is more like a motion picture than a photograph.

As PLTNM-controlled transformations accumulate, current operating conditions become influenced by prior temporal relationships. State transitions matter because they help define how the environment arrives at the condition from which reconstruction is attempted. The protected environment therefore becomes defined not only by where it exists at a moment, but by the sequence of temporal relationships through which it arrived there.

Waveform Evolution And Analog-State Lineage

Temporal state architecture leads naturally to waveform evolution and analog-state lineage. If operating conditions evolve through time, successive states do not exist independently. Each state emerges from conditions established by earlier states while influencing conditions that follow.

Analog-state lineage refers to inherited relationships that connect successive generations of operating states. Carrier dynamics, temporal modulation, waveform conditioning, analog processing structures, and other state-forming mechanisms leave influence on subsequent waveform behavior. The observed waveform is therefore not merely an isolated signal condition; it is the current expression of a transformation history.

This creates an important separation between observation and understanding. An observer may characterize a waveform at a particular moment while remaining unaware of the evolutionary history responsible for producing it. Observation reveals what currently exists. Lineage helps explain how it came to exist.

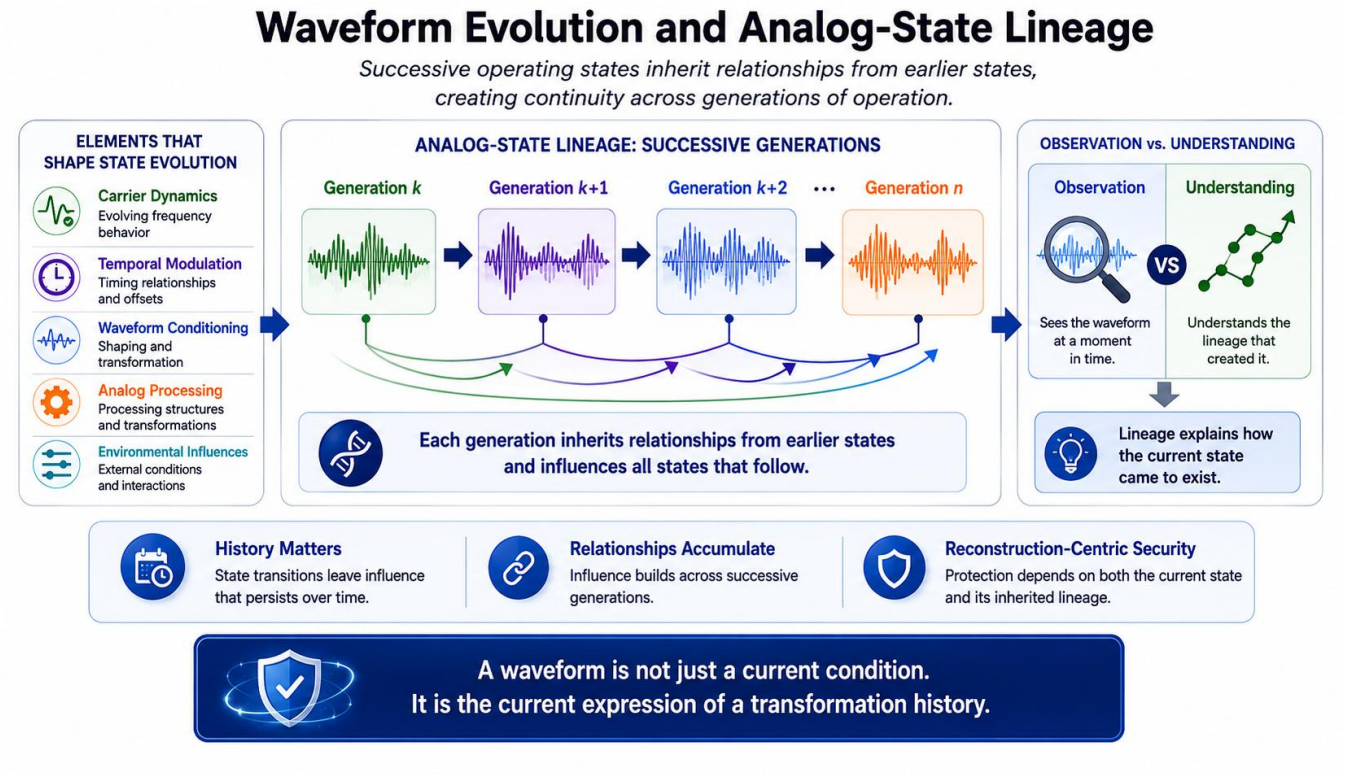

Figure 5 *(Analog-State Lineage and Waveform Evolution) illustrates successive generations of operating states inheriting relationships from earlier transformations.*

As transformation complexity increases, lineage becomes more influential. Current conditions influence future conditions, historical transitions influence later transitions, and relationships accumulate rather than disappear. The protected environment develops continuity across successive generations of operation.

This historical continuity strengthens the transition from conventional encryption toward reconstruction-centric security. The protected environment is no longer defined solely by present operating conditions. It is influenced by inherited relationships that persist across stages of state evolution.

Emergent Analog-State Orchestration

Dynamic carriers, parallel state partitioning, PLTNM, and waveform lineage each contribute to the protected environment. The architecture becomes more powerful when these mechanisms operate simultaneously. At that point, the protected environment can no longer be understood solely by examining individual components. Its behavior increasingly emerges from relationships among participating domains.

This behavior may be described as emergent analog-state orchestration. Emergence occurs when the collective behavior of a system possesses characteristics not fully attributable to any single component acting independently. In Analog Guard®, the resulting state reflects interaction among carrier domains, temporal domains, waveform domains, and partitioned processing environments.

Carrier dynamics may influence temporal evolution. Temporal evolution may influence waveform development. Waveform lineage may influence subsequent state formation. Partitioned domains may influence one another through shared relationships. Each domain contributes to the larger operating environment while responding to conditions established elsewhere in the architecture.

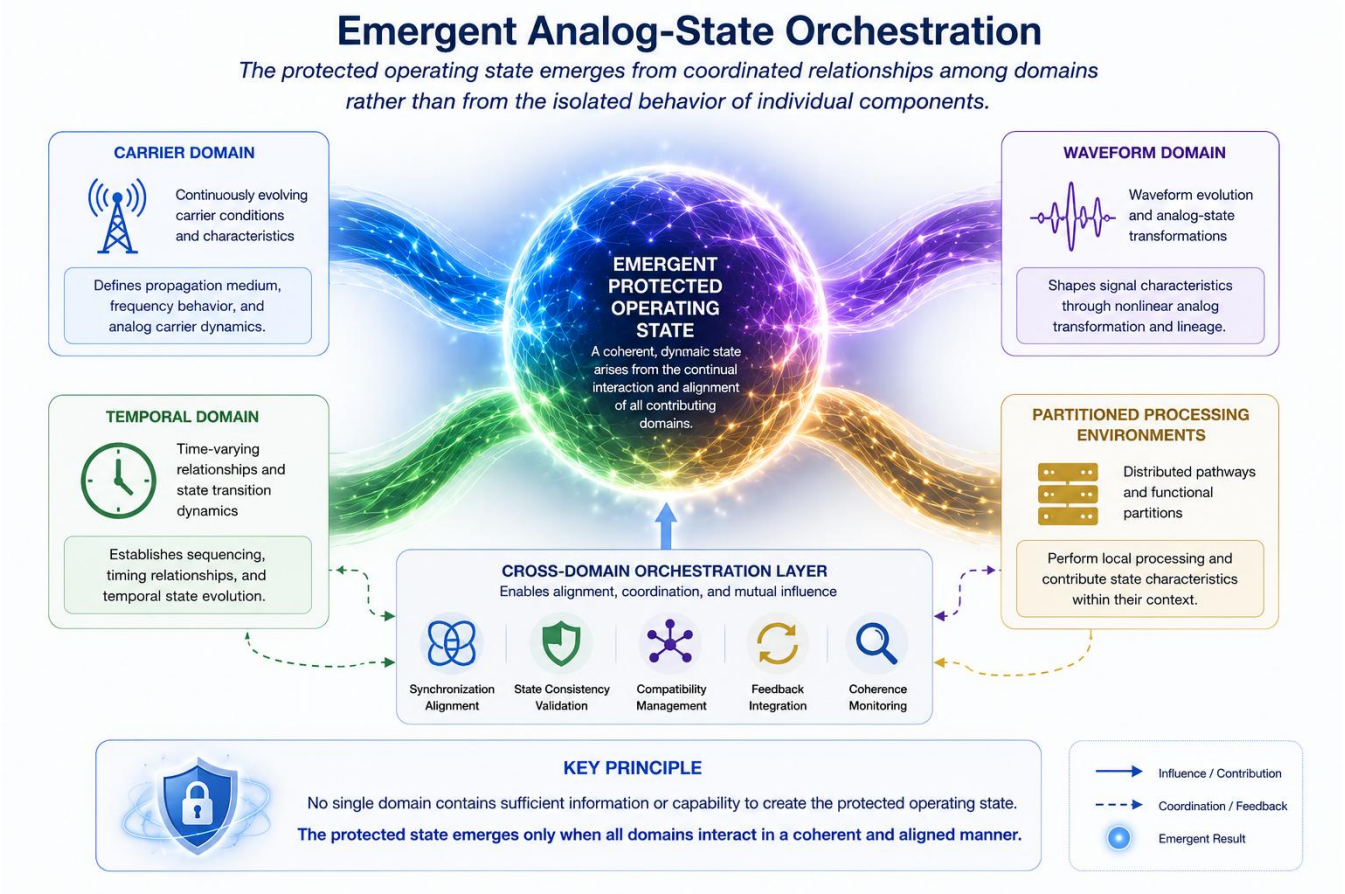

Figure 6 *illustrates carrier, temporal, waveform, and partitioned processing domains producing a system-level protected state.*

The protected environment therefore becomes relational. No individual carrier domain, temporal domain, waveform domain, or processing pathway is required to contain a complete description of the overall operating environment. The protected state exists at the level of coordination rather than at the level of any singular mechanism.

This is the conceptual bridge to DARK. Once reconstruction is understood as emerging from coordinated analog-state relationships rather than from a singular cryptographic condition, the conditions required for reconstruction can be partitioned, distributed, synchronized, governed, and maintained across multiple participating environments.

Reconstruction Dependencies And Authorized Recovery

The preceding sections progressively expand the role of the protected signal. Dynamic carrier environments contribute evolving signal conditions. Parallel pathways partition state. PLTNM introduces temporal architecture. Waveform evolution creates lineage. Multi-domain orchestration produces system-level behavior from relationships among domains.

Together, these mechanisms reveal a central principle: the protected environment is no longer defined solely by encrypted information. It is increasingly defined by the collection of analog-state relationships that influence how information exists, evolves, and may be recovered. That collection of relationships constitutes the reconstruction environment.

The reconstruction environment includes carrier conditions, temporal structures, waveform characteristics, state lineages, transformation histories, synchronization relationships, and inter-domain interactions that collectively influence authorized recovery. Rather than functioning as independent variables, these relationships cooperate to establish the conditions under which reconstruction becomes possible.

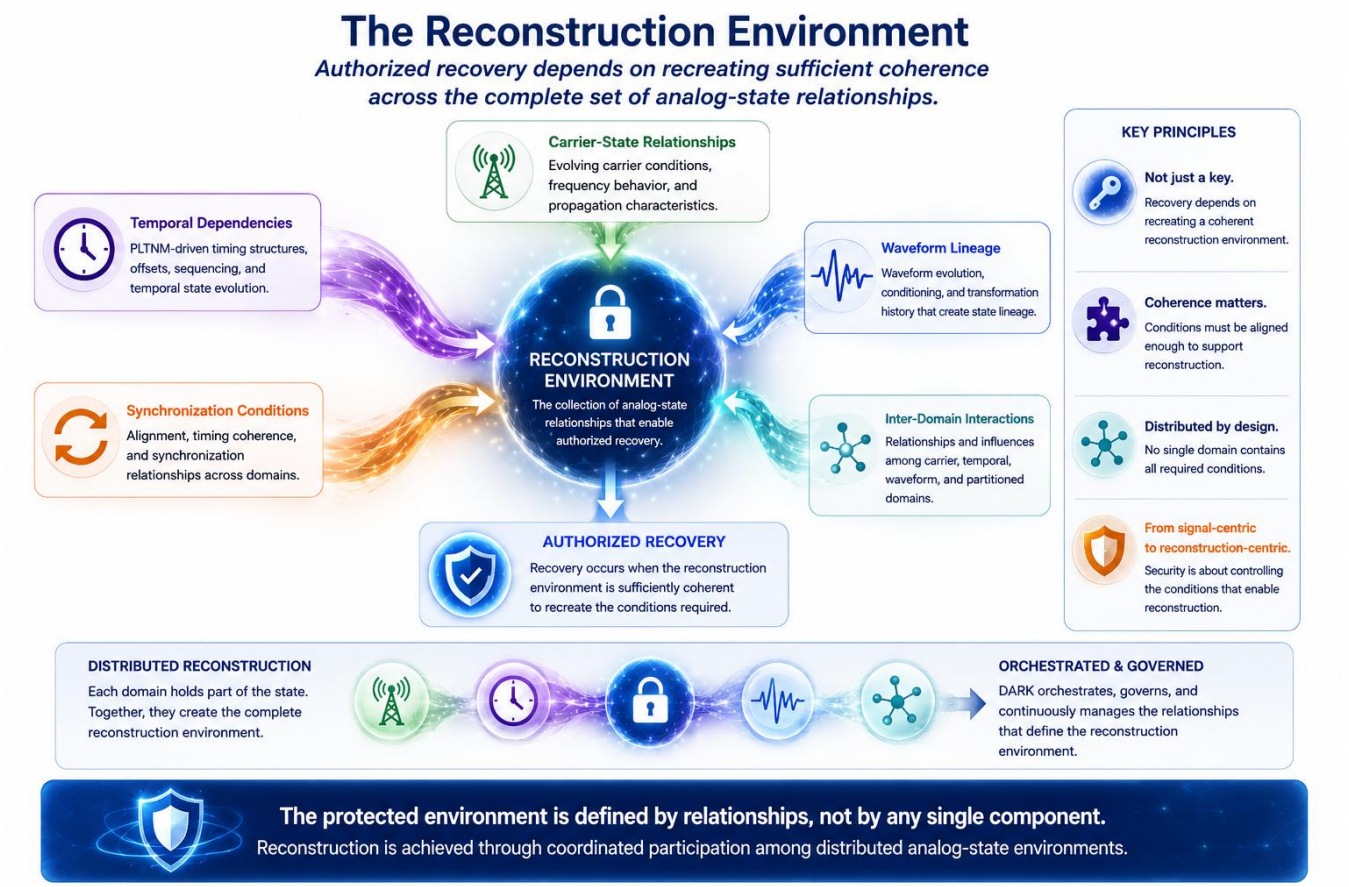

Figure 7 *illustrates carrier-state relationships, temporal dependencies, waveform lineage, synchronization conditions, and inter-domain interactions contributing to authorized recovery.*

This represents a departure from conventional cryptographic thinking. Traditional encryption systems generally assume that possession of the correct key permits recovery of protected information. The physical transport environment may influence reliability, but it is not typically treated as part of the cryptographic state. Within the Analog Guard® framework, recovery increasingly depends upon recreating sufficient coherence across the reconstruction environment.

State coherence refers to the degree to which relationships comprising the reconstruction environment remain sufficiently aligned to support recovery. Carrier behavior, temporal structures, waveform lineage, and domain interactions need not be identical to their original conditions, but they must remain coherent enough to recreate the reconstruction environment required for authorized recovery.

This leads directly to distributed reconstruction. Nothing requires all reconstruction-relevant conditions to reside within one device, pathway, processing domain, or operating environment. Individual domains may contain valid state information while lacking the broader context required to establish a complete reconstruction environment. Each domain may participate in reconstruction without independently containing the complete reconstruction capability.

DARK extends this principle by distributing, orchestrating, governing, and continuously managing the relationships that define the reconstruction environment. The result is a transition from signal-centric protection toward reconstruction-centric security, where the primary objective is to control the conditions under which a valid reconstruction environment can be established.

5. DARK Reconstruction-Key Architecture

From Mixed-Signal Encryption To DARK

Analog Guard® demonstrates that reconstruction capability can emerge from coordinated analog-state conditions. DARK governs how those operating relationships are partitioned among participating authorities, how compatibility is maintained across distributed environments, how participation is controlled, and how a coherent recovery environment is established under authorized conditions.

Within DARK, the term reconstruction-key refers to the distributed collection of analog-state conditions, synchronization relationships, validation states, lineage dependencies, replay-domain participation conditions, and governance mechanisms whose coordinated interaction enables authorized reconstruction. The reconstruction-key is therefore not a singular stored credential. It is a distributed recovery capability established through authorized participation across multiple domains.

This distinction changes the focus of security. Recoverability becomes influenced by coordinated management of distributed conditions rather than by protection of a singular credential or recovery artifact. The system treats recovery as a governed process occurring within a managed reconstruction environment whose participating elements remain independently maintained while collectively supporting authorized operation.

DARK is therefore not a replacement for Analog Guard®. It is the distributed operational architecture built upon the reconstruction principles that Analog Guard® establishes. Analog Guard® demonstrates how reconstruction-relevant relationships can be created. DARK governs how those relationships are distributed, synchronized, validated, authorized, and invalidated throughout a distributed recovery environment.

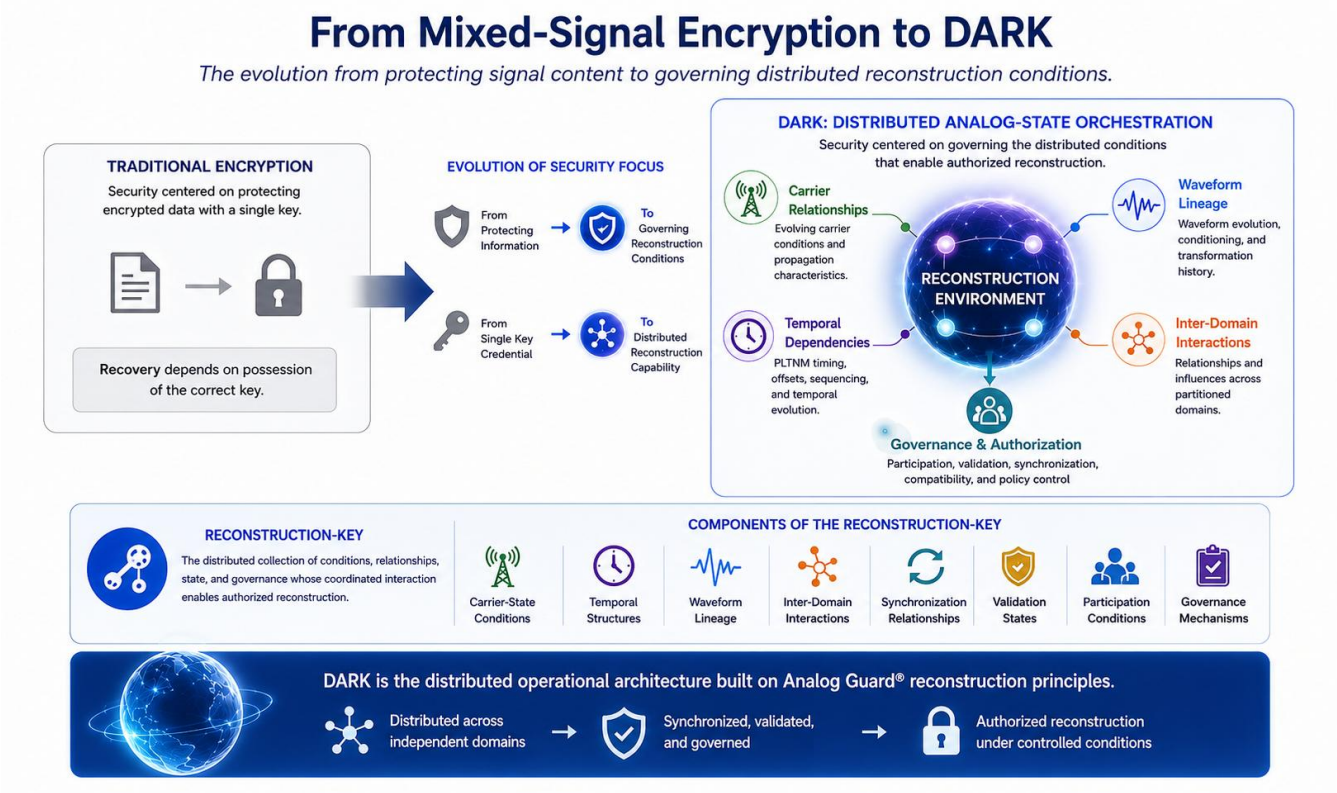

Figure 8 *illustrates the transition from signal protection toward governance of distributed reconstruction conditions.*

In the Analog Guard discussion, the article refers broadly to analog-state conditions, carrier relationships, temporal dependencies, waveform lineage, and reconstruction-environment coherence. DARK generalizes those reconstruction-relevant conditions into replay domains. A replay domain may therefore be understood as a separately maintained operational condition that participates in synchronized reconstruction. This terminology allows DARK to describe not only analog waveform conditions, but also timing, synchronization, routing, transport, authorization, validation, and governance conditions that collectively determine whether reconstruction can occur.

Distributed Replay-domain Custody

In DARK, distributed analog-state custody is refined into replay-domain custody. A replay domain is a separately maintained operational component that participates in synchronized replay interaction. It may contribute a waveform component, timing component, synchronization component, transport component, control component, authorization component, reconstruction component, or combination of such conditions.

The important point is not merely where information resides, but which operational condition each participant maintains. A replay-domain custody environment may maintain only an operationally incomplete participation component. That component may be valid and necessary, but it does not independently satisfy reconstruction criteria outside active synchronized replay participation.

Traditional key custody concerns safeguarding a discrete object whose possession enables authorized operation. Replay-domain custody concerns stewardship of operating relationships that collectively contribute to reconstruction. A domain may maintain synchronization relationships, another may maintain temporal continuity, another may maintain carrier-state conditions, another may maintain validation structures, and another may maintain operational policies.

Custody therefore means responsibility rather than possession. Each participating domain preserves the integrity of the responsibilities under its authority while maintaining compatibility with the broader reconstruction environment. The resulting framework resembles a distributed governance system more than a traditional key-management architecture.

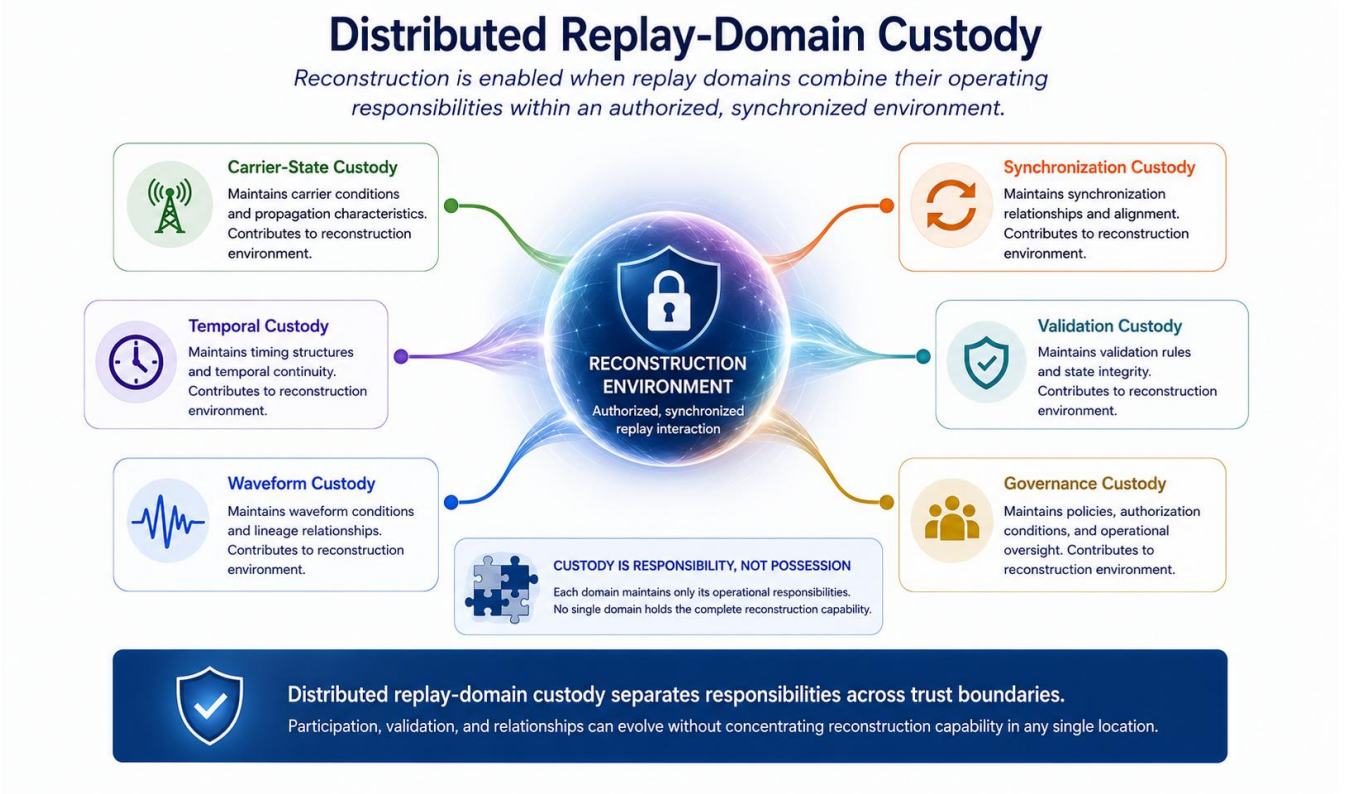

Figure 9 *depicts reconstruction responsibilities distributed among custodial authorities, each maintaining only part of the operating environment.*

Distributed custody allows responsibilities to be separated according to trust boundaries, organizations, facilities, devices, or administrative authorities. Participation rules may change, validation requirements may adapt, and operational relationships may be reconfigured without requiring reconstruction capability to be concentrated in a single location.

Synchronization-governed Reconstruction

Distributed replay-domain custody alone does not guarantee successful reconstruction. Custody domains may preserve their assigned responsibilities while evolving independently over time. Temporal conditions may diverge, validation states may change, policies may be updated, and local environments may develop differently. The broader reconstruction architecture can therefore lose alignment even when each domain remains internally consistent.

DARK treats synchronization continuity as a reconstruction-governance dependency rather than merely a communications convenience. Synchronization does not simply coordinate when participants exchange information. It helps determine whether replay-domain participation components are compatible enough to establish reconstruction capability inside replay-isolated hardware.

State alignment refers to the process through which synchronized participants maintain the operating relationships necessary to support reconstruction. The objective is not necessarily to force all participants into identical conditions. Rather, the objective is to preserve sufficient alignment among distributed participants to allow the reconstruction architecture to function as intended.

Synchronization governance encompasses the policies, mechanisms, validation procedures, and coordination processes used to manage that alignment. These mechanisms determine when synchronization must occur, how alignment is evaluated, what constitutes acceptable deviation, and under what conditions participation remains valid.

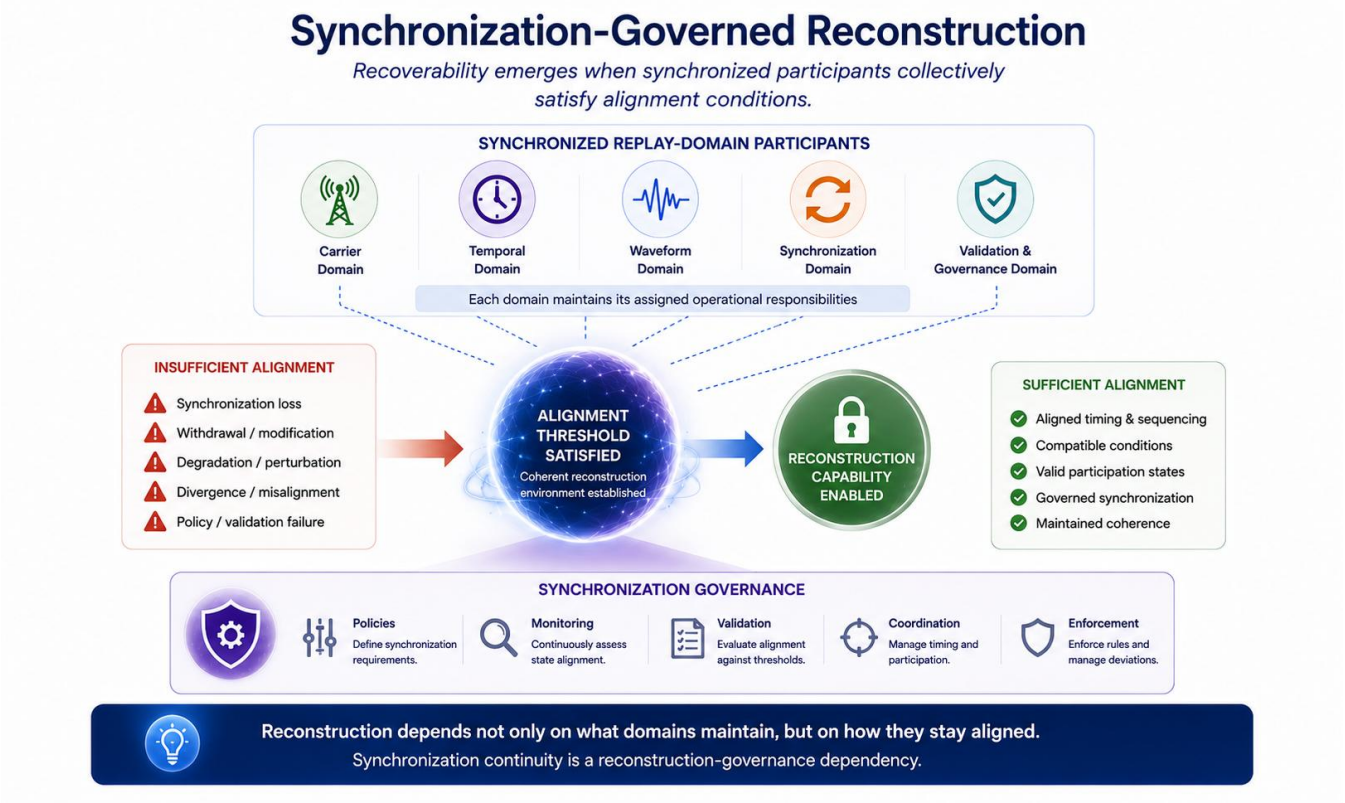

Figure 10 *illustrates recoverability emerging when synchronized participants collectively satisfy alignment conditions.*

Because synchronization participates in reconstruction governance, synchronization loss, withdrawal, modification, degradation, perturbation, or divergence may trigger replay invalidation, anti-stabilization, entropy divergence,

replay-state orphaning, topology mutation, or replay collapse. Reconstruction becomes dependent not only on what participating domains maintain, but also on how those domains remain aligned as they evolve.

6. Governance, Evaluation, and Invalidation

Replay-Isolated Hardware And Physical Replay Invalidation

Replay-isolated hardware is the environment in which the distinction between abstract authorization and physical reconstruction governance becomes clearest. It refers to a hardware-confined reconstruction environment separated from generalized software-processing environments, persistent replay-state storage pathways, and non-participating computational resources.

Within such hardware, replay-domain participation components may be introduced only during bounded replay intervals. The components may include waveform components, timing references, synchronization conditions, replay-buffer states, replay-routing relationships, transport states, authorization states, validation states, or governance conditions. None of these components, considered independently, is sufficient to establish authorized reconstruction.

This hardware-centered framing prevents DARK from being reduced to a software authorization rule. The architecture is not merely deciding whether a user is allowed to access a stored secret. Replay-governance circuitry may cause physical modification of the reconstruction environment itself.

Representative physical operations include replay-buffer invalidation, synchronization-reference withdrawal, synchronization-reference modification, timing-offset introduction, routing-fabric reconfiguration, replay-pathway reassignment, replay-domain isolation, waveform perturbation, phase perturbation, optical-path isolation, wavelength-channel reassignment, and authorization-control modification.

These operations may be triggered when replay-state indicators fail to satisfy replay-coordination criteria, when synchronization continuity is interrupted, when replay stabilization persists beyond an authorized condition, or when authorization or attestation fails. The resulting hardware-state change can prevent residual replay-domain fragments from reattaching to the timing, phase, routing, waveform-conditioning, transport, or authorization relationships required for reconstruction.

Reconstruction Governance And Coherence Evaluation

DARK uses a concrete evaluation framework for reconstruction governance. Replay compatibility and reconstruction authorization may be determined by replay-governance circuitry, coherence-determination circuitry, reconstruction-authorization circuitry, validation circuitry, hardware-attestation infrastructure, or combinations of these components.

Representative replay-state and coherence indicators include timing deviation, replay jitter, phase deviation, waveform correlation, waveform coherence, spectral divergence, replay-buffer occupancy, replay-routing state, synchronization-reference state, transport-state condition, authorization-state condition, environmental condition, hardware-attestation condition, and replay-domain participation condition. These indicators may be compared against fixed, adaptive, statistically derived, policy-controlled, hardware-controlled, machine-learned, or dynamically updated thresholds.

Coherence may represent the degree to which participating domains maintain relationships necessary to support authorized reconstruction. Such relationships may include synchronization conditions, analog-state conditions, temporal-state conditions, waveform lineage conditions, validation states, compatibility relationships, governance policies, operational histories, environmental dependencies, or combinations thereof.

Multiple evaluation mechanisms may be used. Synchronization-based evaluation considers timing relationships, state continuity, operational consistency, and participation status. Compatibility-based evaluation considers relationships among analog-state conditions, temporal dependencies, lineage characteristics, validation structures, governance policies, and environmental conditions. Threshold-based evaluation permits reconstruction when one or more coherence metrics satisfy applicable criteria.

Weighted evaluation allows different domains or authorities to contribute different levels of influence. Quorum-based evaluation may require participation by a minimum number of authorized entities. Consensus-based evaluation may require coordinated approval, validation, acknowledgment, or participation among multiple governance authorities. Analog-state correlation, temporal persistence, and multi-domain relationship evaluation may also be used.

No single coherence metric is required. The central principle is that reconstruction capability emerges through coordinated evaluation of distributed relationships rather than through possession, storage, transmission, reconstruction, or protection of a singular recoverable key, credential, artifact, or recovery object.

Replay Compatibility And Non-Equilibrium States

Replay compatibility is an operational condition in which two or more replay domains satisfy replay-coordination criteria sufficient to permit synchronized replay interaction within replay-isolated reconstruction hardware. It is not a permanent possession state. It is a transient condition that may exist only while participating replay domains remain coordinated during a bounded replay interval.

The non-equilibrium nature of the architecture is central. Replay compatibility may require ongoing synchronized replay-domain participation, active synchronization continuity, continuously maintained replay coordination relationships, and continuously maintained replay-governance conditions to remain operationally sustainable.

This leads to an important question: if a recovery framework has previously supported successful reconstruction, can that same operating state be reused indefinitely? In static credential systems, the answer may often depend on whether the credential is still valid. In DARK, the answer depends on whether prior operating conditions remain sufficiently compatible with the current reconstruction environment.

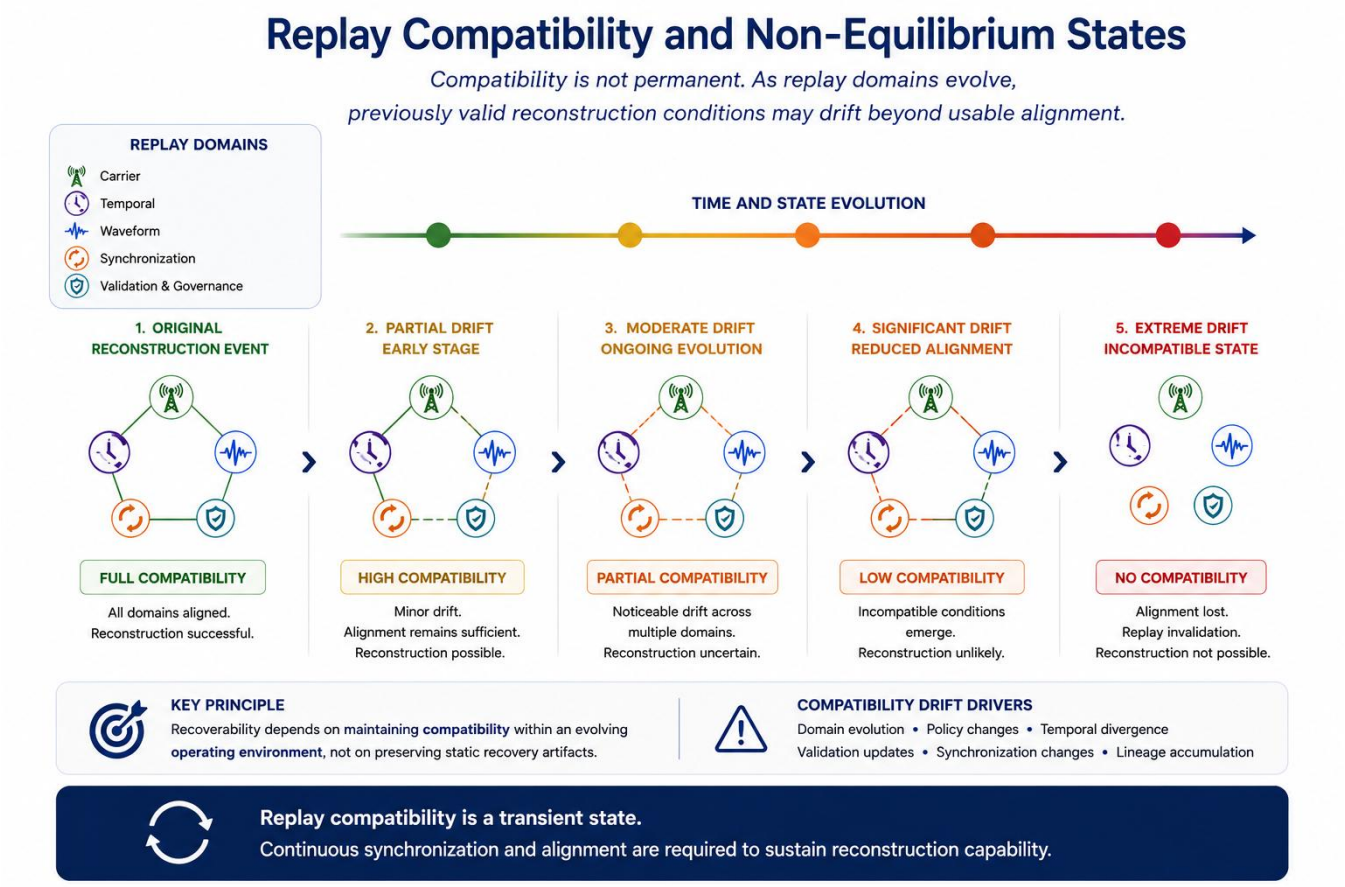

Figure 11 *illustrates how previously valid reconstruction conditions may lose compatibility as participating domains evolve.*

As custody domains evolve, temporal structures continue developing, validation conditions change, synchronization dependencies adapt, and state lineage accumulates. A previously valid recovery state may retain substantial compatibility, partial compatibility, or little useful compatibility depending on how the operational domains have evolved since the original reconstruction event.

Replay compatibility therefore exists along a continuum. A historical state may be perfectly preserved, yet no longer possess sufficient compatibility with current conditions to support reconstruction. The limitation arises not from data loss, but from compatibility drift and ongoing state evolution.

This emphasis on compatibility rather than preservation departs from traditional security models. Recoverability increasingly emerges from maintaining compatibility within an evolving operating environment rather than preserving static recovery artifacts. As compatibility drift accumulates, incompatibilities may begin propagating across the broader reconstruction architecture.

Anti-stabilization And Incompatibility Propagation

Anti-stabilization is hardware-governed behavior that inhibits formation or persistence of replay compatibility outside authorized synchronized replay participation. The concept is tied to measurable indicators, thresholds, and specific hardware operations rather than merely to a descriptive preference for variability.

Anti-stabilization may be triggered when waveform-correlation persistence, waveform-coherence persistence, phase-lock persistence, replay repeatability, replay-buffer persistence, replay-routing-state persistence, topology-state persistence, transport-state consistency, authorization-state persistence, or replay compatibility persistence satisfies a stabilization threshold or persistence condition outside an authorized replay state.

In many conventional systems, divergence is treated primarily as an operational problem, and stability is usually desirable. DARK treats persistent stability more carefully. A perfectly stable operating state may become predictable, reusable, and modelable. DARK instead seeks an operating condition that remains coherent enough for authorized reconstruction without converging toward an indefinitely reusable equilibrium.

When divergence develops in one portion of the environment, its effects may propagate. A timing deviation may affect synchronization dependencies; modified synchronization conditions may affect validation behavior; validation changes may affect participation status; participation changes may affect broader replay compatibility. This is incompatibility propagation.

For example, a timing deviation in one replay domain may cause a phase relationship to fall outside an allowed threshold. That phase deviation may cause waveform correlation to degrade, which may then cause replay-governance circuitry to withdraw a synchronization reference, invalidate a replay buffer, or reassign a replay pathway. The result is not merely denial of access; the reconstruction environment itself changes so that residual replay-domain fragments cannot easily reattach into a stable compatible state.

Incompatibility propagation does not imply immediate failure. The architecture may tolerate limited divergence while remaining capable of authorized operation. However, as divergence accumulates, its effects may progressively influence larger portions of the reconstruction environment, resulting in replay-state orphaning, entropy divergence, topology mutation, or replay collapse.

Anti-stabilization and incompatibility propagation therefore function together. Anti-stabilization discourages long-term convergence toward a permanently reusable condition. Incompatibility propagation ensures that divergence affects the reconstruction environment as a governed system-level behavior rather than remaining isolated within a single domain.

Figure 12. Controlled Evolution and Anti-Stabilization

ıe system maintains coherence during authorized replay while inhibiting persistent replay compatibility outside the authorized interv. When stabilization or divergence crosses a threshold, replay-governance circuitry physically changes the reconstruction environment

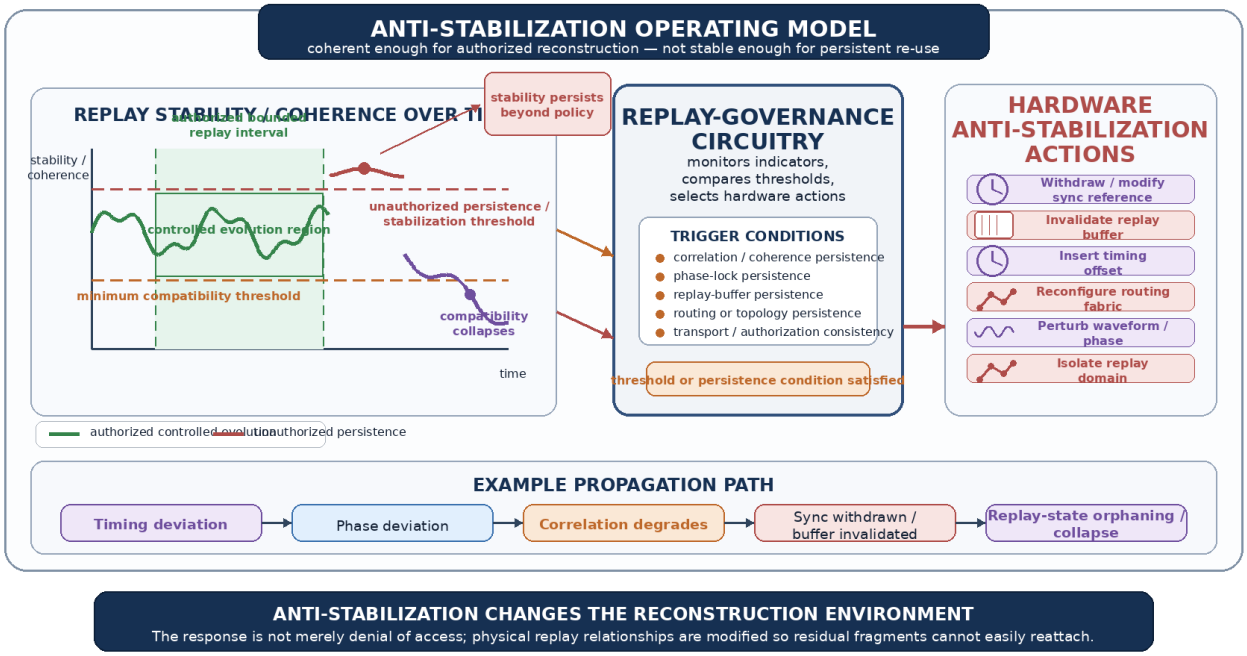

***Figure 12** illustrates coherence maintained without long-term convergence toward static operating conditions.*

7. Representative Implementation Models

Representative DARK Implementation Architectures

The DARK architecture can be embodied through multiple concrete implementation architectures. These are not mutually exclusive. A deployed system may combine FPGA/DAC timing control, analog or mixed-signal waveform conditioning, distributed node governance, SDR interfaces, optical or photonic transport, hardware attestation, and replay-governed invalidation within a single architecture.

FPGA/DAC Deterministic-latency Replay

In an FPGA/DAC deterministic-latency embodiment, replay-domain participation components may be staged in FPGA block RAM, FIFO memory, distributed RAM, shift-register logic, or dedicated buffer circuitry. Synchronization-control logic establishes a bounded replay window, and replay-buffer controllers release participation components according to deterministic timing relationships. DAC resources convert released components into analog replay waveforms that are routed through waveform-conditioning circuitry.

Replay-validation logic may evaluate timing deviation, replay jitter, phase deviation, waveform correlation, waveform coherence, spectral divergence, replay-buffer occupancy, replay-routing state, synchronization-reference state, and authorization-state condition. If criteria are not satisfied, replay-governance logic may purge buffers, overwrite contents, disable buffer read-enable signals, modify buffer pointers, insert timing offsets, withdraw synchronization references, alter DAC update timing, reconfigure FPGA routing fabric, isolate replay pathways, or perturb waveform-conditioning parameters.

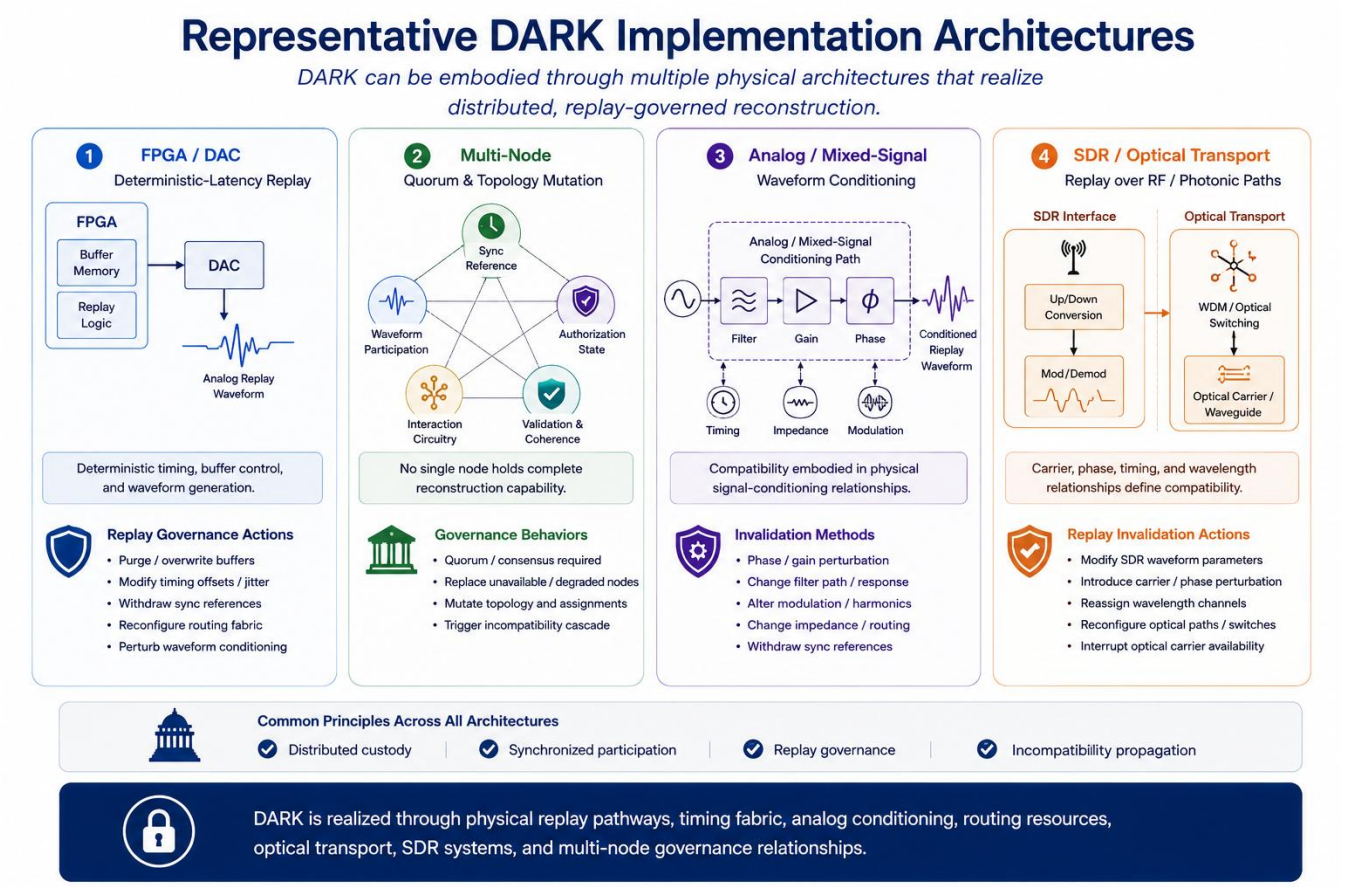

Figure 13 *(Representative DARK Implementation Architectures) illustrates FPGA/DAC, multi-node, analog/mixed-signal, and SDR/optical implementations as examples of the broader architecture.*

Multi-Node Quorum And Topology Mutation

In a multi-node embodiment, reconstruction capability may be distributed across geographically or logically separated nodes. One node may maintain synchronization-reference information, another may maintain waveform-participation behavior, another may maintain analog or mixed-signal interaction circuitry, another may maintain authorization state, and another may maintain validation or coherence-evaluation logic. No individual node independently possesses a complete reconstruction-key.

Authorized operation may require quorum, consensus, coherence, hardware-attestation, and compatibility criteria. If a node becomes unavailable, degraded, unauthorized, or untrusted, replay-governance circuitry may either mutate topology by assigning a replacement node or initiate incompatibility cascade behavior. Topology mutation may reassign replay transport pathways, synchronization responsibilities, waveform-interaction roles, replay-buffer responsibilities, or authorization relationships while preserving distributed custody.

Analog Or Mixed-Signal Waveform Conditioning

In an analog or mixed-signal embodiment, replay compatibility may be physically embodied in transient waveform-conditioning relationships. Participating conditions may include timing relationships, phase or carrier relationships, gain conditions, filter conditions, modulation conditions, harmonic relationships, impedance states, waveform-shaping relationships, authorization states, and governance states.

Replay invalidation may be implemented by changing physical signal-conditioning relationships. Representative actions include introducing phase perturbation, changing gain state, changing filter path or response, modifying modulation relationships, altering harmonic-conditioning behavior, changing impedance state, switching analog pathways, disabling analog switches, perturbing DAC update relationships, modifying ADC sampling relationships, or withdrawing synchronization references coupled to analog waveform-conditioning circuitry.

SDR And Optical Transport Replay

In an SDR/optical transport embodiment, replay compatibility may depend upon synchronized carrier, phase, timing, waveform, wavelength, and optical transport relationships. A software-defined radio replay interface may generate or condition replay waveforms using numerically controlled oscillators, digital upconversion, digital downconversion, quadrature modulation, carrier tracking, programmable filtering, or waveform synthesis logic.

Optical or photonic transport circuitry may route replay-domain participation through wavelength-separated pathways, optical carriers, photonic waveguides, free-space optical pathways, optical switching fabric, wavelength-division multiplexing infrastructure, or optical transport interfaces. Replay invalidation may occur by modifying SDR waveform-generation parameters, introducing carrier or phase perturbation, withdrawing synchronization references, changing wavelength-channel assignments, reassigning optical transport pathways, disabling optical modulators, opening or closing optical switches, isolating photonic waveguides, or interrupting optical carrier availability.

Together, these implementation architectures demonstrate that DARK is not limited to a generic software authorization framework. The architecture may be embodied in physical replay pathways, deterministic timing fabric, analog signal-conditioning circuits, FPGA routing resources, optical switching structures, SDR waveform-generation systems, and multi-node replay-governance relationships.

Multi-Node Distributed Reconstruction

Multi-node reconstruction is both a representative implementation architecture and a broader deployment model. Reconstruction nodes may maintain different partial reconstruction conditions, including synchronization-reference information, waveform-participation behavior, replay-domain custody, analog or mixed-signal interaction circuitry, authorization state, validation state, coherence-evaluation logic, hardware-attestation state, or governance state.

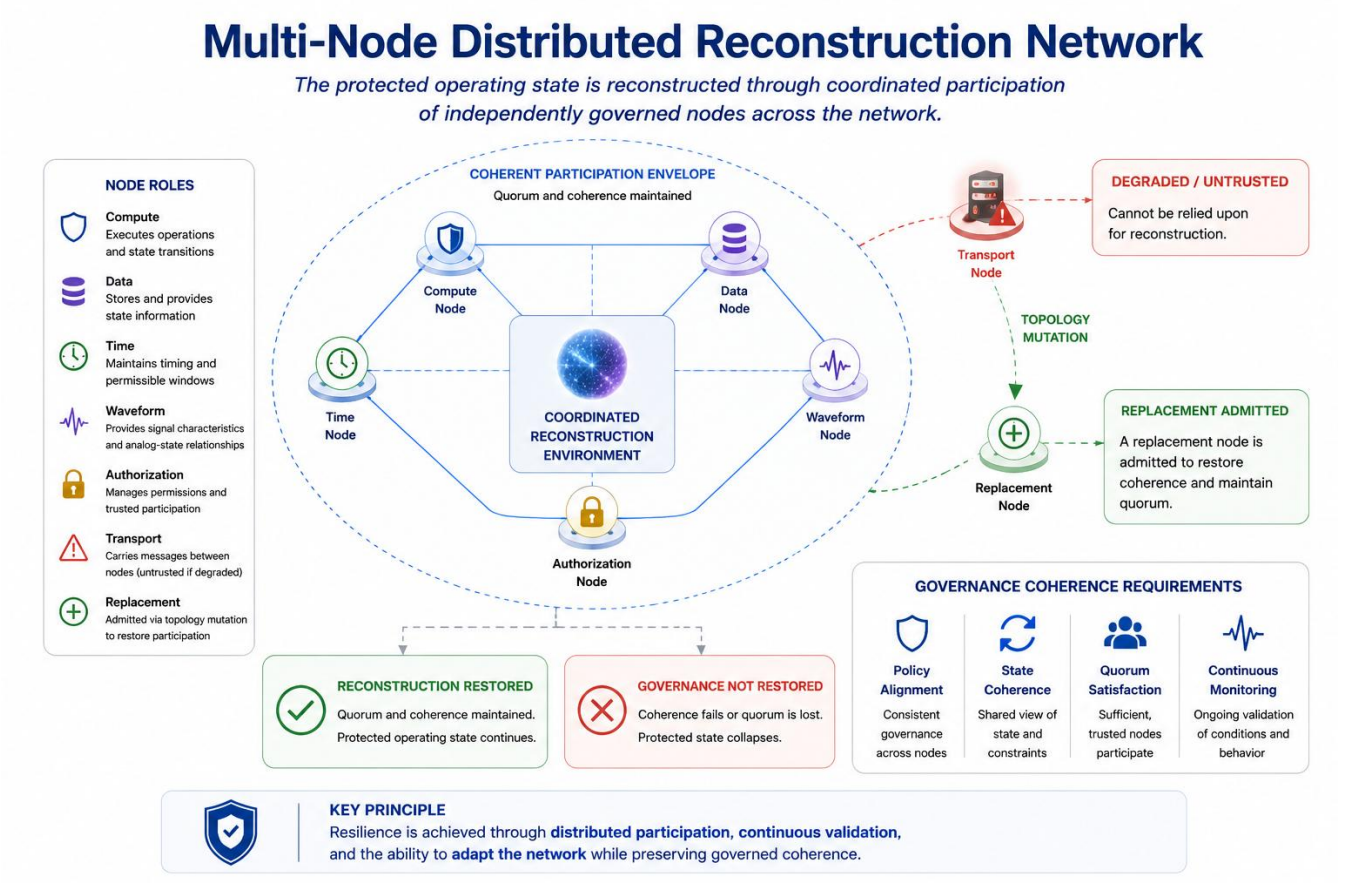

Figure 14 *(Multi-Node Distributed Reconstruction Network) illustrates reconstruction capability emerging through coordinated participation among independently governed nodes.*

Authorized reconstruction may require quorum, consensus, coherence, authorization, compatibility, and hardware-attestation criteria. If a node becomes unavailable, isolated, degraded, destabilized, unauthorized, or untrusted, the system may either mutate the replay topology to assign replacement participation roles or initiate incompatibility cascade behavior leading to replay invalidation and collapse.

As the number of reconstruction nodes grows, recoverability becomes increasingly distributed. No individual participant is responsible for producing recovery independently. Some nodes may maintain synchronization dependencies, others may support validation, others may preserve lineage continuity, and others may govern policy, environmental conditions, or compatibility requirements.

This allows the architecture to scale through participation rather than centralization. Network topology may change, nodes may be added, validation authorities may be reassigned, and synchronization mechanisms may adapt while the architecture continues operating so long as the required distributed relationships remain available.

The protected capability increasingly resides within the architecture itself rather than within any individual component. This leads directly to one of the most important implications of DARK: if reconstruction emerges through coordinated interaction among distributed participants, no complete recovery capability needs to exist in any single location.

8. Distributed Reconstruction and Strategic Implications

Why No Complete Key Exists Anywhere

Within DARK, the reconstruction-key concept does not refer to a singular recoverable cryptographic key. A reconstruction-key is a distributed collection of replay-domain participation conditions, synchronization relationships, replay-governance relationships, waveform interaction conditions, reconstruction dependencies, validation conditions, operational states, environmental conditions, authorization relationships, or combinations thereof whose coordinated interaction enables authorized reconstruction.

Modern cryptographic systems are built upon the assumption that complete recoverability exists somewhere within the architecture. A key may reside within a hardware security module, be protected by access controls, be divided through secret-sharing mechanisms, or be stored within secured facilities. However implemented, the model assumes that a complete recovery capability exists and must be protected.

DARK challenges that assumption. The architecture does not require a complete key, complete share set, complete recovery artifact, or complete reconstruction state to exist in any individual location. Reconstruction capability exists as an emergent property of coordinated distributed replay participation, and it may cease to exist as an operational capability when replay compatibility collapses.

This separates DARK from conventional distributed key management. Many distributed cryptographic systems divide a key into fragments while preserving the assumption that the complete key can ultimately be reconstructed when sufficient fragments are combined. DARK does not merely fragment a key. It does not require a complete key as a prerequisite for operation.

The result is a different security model. Compromise of an individual custody authority, synchronization authority, validation authority, reconstruction node, transport pathway, or waveform region does not reveal a complete recovery capability. An observer may obtain local governance relationships while remaining unable to establish the broader reconstruction environment necessary for recovery.

The protected asset is therefore not a key. The protected asset is the ability to create the circumstances under which reconstruction becomes possible. Security shifts from concealment of a stored secret to governance of the distributed relationships that transiently enable reconstruction.

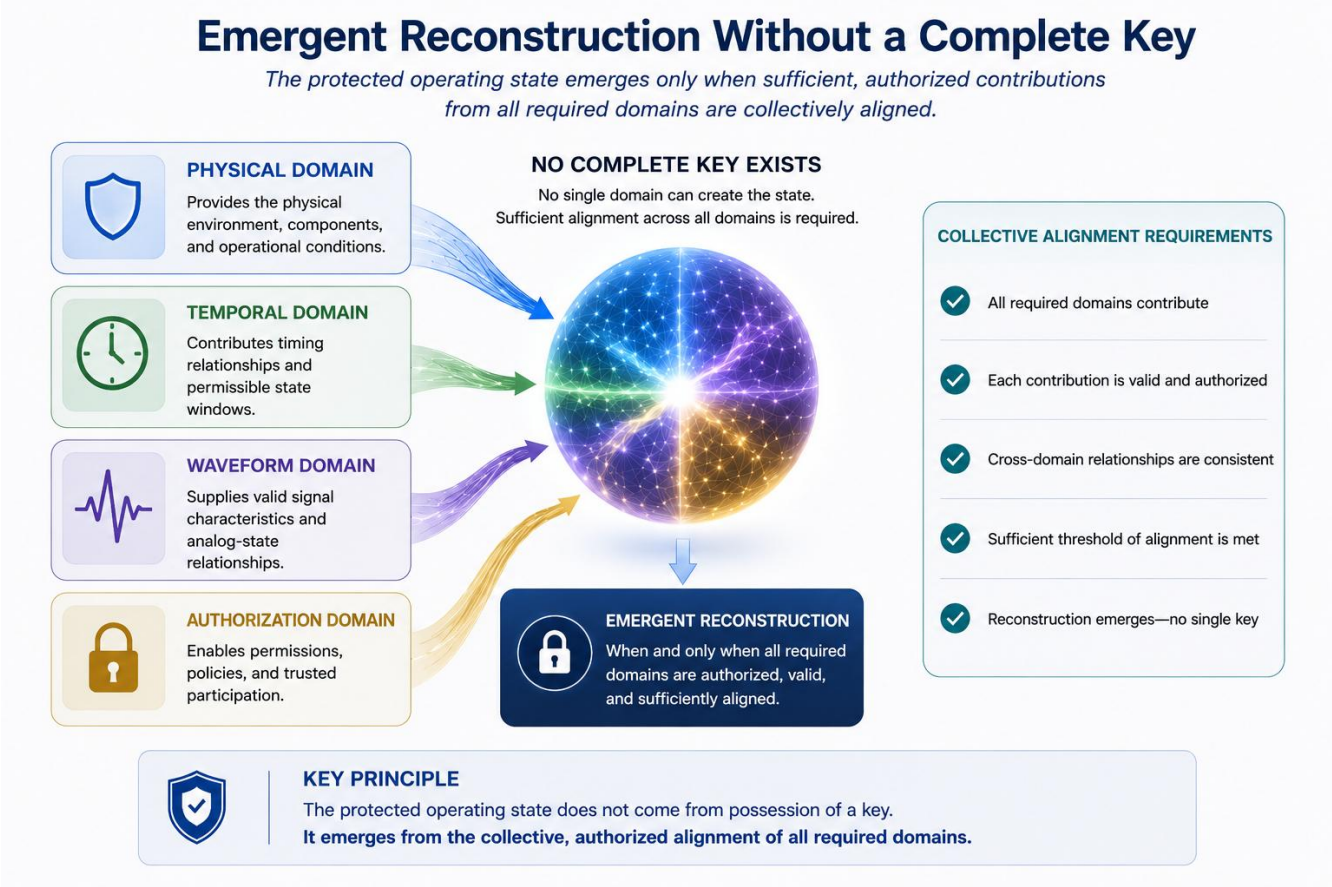

Figure 15 *(Emergent Reconstruction Capability Without a Complete Key) illustrates recovery capability emerging only when distributed relationships align sufficiently.*

Implications For Model-Assisted Analysis, Quantum, And The Future Of Cybersecurity

Future cybersecurity will likely be shaped by increasingly capable analytical systems. Artificial intelligence, model-assisted signal analysis, autonomous cyber tools, large-scale behavioral modeling, and future computational methods may improve the ability of adversaries to identify patterns, infer relationships, classify transmission behavior, and search for persistent structures within complex systems.

DARK should not be described as immune to those methods. No serious security architecture should assume immunity from artificial intelligence, quantum computing, advanced signal analysis, insider compromise, or future analytical techniques. The more defensible point is narrower and stronger: DARK changes the object that those methods must analyze.

In a conventional key-centric architecture, an adversary often seeks a recoverable object or a stable derivation process. The target may be a key, key share, credential, token, secret, PUF response, stored artifact, or authorization pathway. Even when the object is well protected, the model assumes that a recoverable capability exists somewhere within the architecture.

In DARK, the target is not merely a stored object. It is a transient reconstruction condition formed from distributed replay-domain participation, synchronization continuity, replay-governance evaluation, waveform interaction, transport state, authorization state, and replay-isolated hardware behavior. Reconstruction capability exists only while those relationships satisfy replay-coordination criteria during an authorized bounded replay interval.

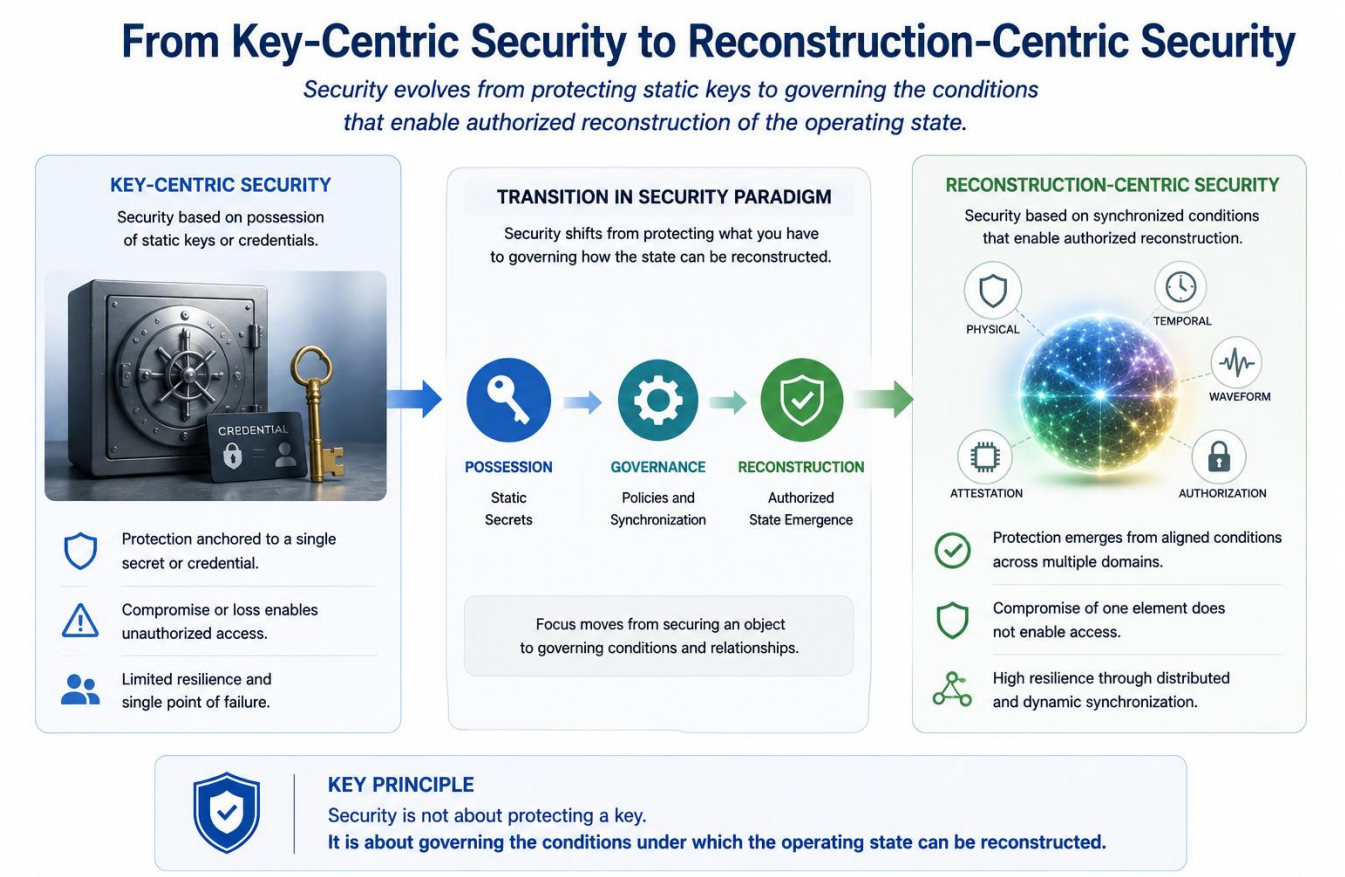

Figure 16 *(From Key-Centric Security to Reconstruction-Centric Security) contrasts protection of recoverable artifacts with governance of reconstructability conditions.*

This can make the analytical problem less like discovering a static secret and more like reconstructing a moving hardware-governed operating condition. A model-assisted adversary would need to account for timing deviation, replay jitter, phase deviation, waveform correlation, waveform coherence, spectral divergence, replay-buffer state, routing state, synchronization-reference state, transport state, authorization state, topology mutation, and replay collapse behavior.

Quantum computing raises a different but related issue. Much post-quantum work focuses on mathematical algorithms intended to resist future computational attacks, and that work remains essential. DARK does not replace post-quantum cryptography. It addresses a complementary architectural dimension by reducing reliance on a singular recoverable secret as the sole basis for reconstruction.

The broader implication is that cybersecurity may increasingly combine algorithmic strength with reconstruction governance. Strong algorithms will remain important, but future systems may also need to control the physical, temporal, synchronization, and governance conditions under which protected information can become recoverable.

Viewed in this broader context, Analog Guard® and DARK represent a shift from key-centric security toward reconstruction-centric security. The objective is not simply to protect a secret. The objective is to govern when, where, and under what conditions reconstruction capability can transiently emerge, and to ensure that the conditions supporting reconstruction collapse or become non-reattachable when authorization, synchronization, or replay-coordination criteria fail.

9. Conclusion

Analog Guard® and DARK are best understood as complementary parts of a reconstruction-centric security architecture. Analog Guard® shows how physical signal behavior, temporal modulation, carrier evolution, waveform lineage, and analog-state dependencies can become part of the conditions required for authorized recovery. DARK extends that principle by distributing those reconstruction-relevant conditions across replay domains and governing their synchronized participation.

The central shift is from protecting a recoverable object to governing reconstructability itself. In DARK, reconstruction capability can be transient, conditional, hardware-bound, and dependent upon distributed replay compatibility. When synchronization, authorization, coherence, or replay-coordination criteria fail, the system may physically alter the replay environment so that compatibility collapses rather than persists as a reusable recovery state.

This does not eliminate the need for strong cryptographic algorithms, hardware security, access control, or post-quantum techniques. Instead, it adds another architectural layer: control over the physical, temporal, synchronization, and governance conditions under which protected information can become recoverable. In that sense, DARK reframes the protected asset as the governed ability to establish reconstruction conditions, not merely the possession of a stored secret.

Appendix A. Figure Inventory

Figure	Description
Figure 1	conceptually illustrates this principle. The figure shows reconstruction capability emerging when carrier conditions, temporal relationships, waveform lineage, and synchronization dependencies remain sufficiently coherent. As those conditions diverge, reconstruction performance degrades, emphasizing that recoverability depends upon environmental coherence rather than possession of information alone.
Figure 2	(Dynamic Carrier Environment) conceptually illustrates carrier evolution as an active contributor to the protected analog-state environment rather than merely a transport mechanism.
Figure 3	illustrates multiple pathways contributing local state characteristics while participating in a broader reconstruction environment.
Figure 4	illustrates successive operating states evolving through controlled temporal transitions.
Figure 5	(Analog-State Lineage and Waveform Evolution) illustrates successive generations of operating states inheriting relationships from earlier transformations.
Figure 6	illustrates carrier, temporal, waveform, and partitioned processing domains producing a system-level protected state.
Figure 7	illustrates carrier-state relationships, temporal dependencies, waveform lineage, synchronization conditions, and inter-domain interactions contributing to authorized recovery.
Figure 8	illustrates the transition from signal protection toward governance of distributed reconstruction conditions.
Figure 9	depicts reconstruction responsibilities distributed among custodial authorities, each maintaining only part of the operating environment.
Figure 10	illustrates recoverability emerging when synchronized participants collectively satisfy alignment conditions.
Figure 11	illustrates how previously valid reconstruction conditions may lose compatibility as participating domains evolve.
Figure 12	illustrates coherence maintained without long-term convergence toward static operating conditions.
Figure 13	(Representative DARK Implementation Architectures) illustrates FPGA/DAC, multi-node, analog/mixed-signal, and SDR/optical implementations as examples of the broader architecture.
Figure 14	(Multi-Node Distributed Reconstruction Network) illustrates reconstruction capability emerging through coordinated participation among independently governed nodes.
Figure 15	(Emergent Reconstruction Capability Without a Complete Key) illustrates recovery capability emerging only when distributed relationships align sufficiently.
Figure 16	(From Key-Centric Security to Reconstruction-Centric Security) contrasts protection of recoverable artifacts with governance of reconstructability conditions.

Appendix B. Key Terms

Term	Working Definition
Analog Guard®	A mixed-signal physical-layer encryption framework in which physical signal behavior, temporal modulation, carrier evolution, waveform lineage, and analog-state dependencies participate in protection and recovery.
DARK	The Distributed Analog Reconstruction-Key System; a synchronization-governed replay coordination architecture built on Analog Guard® reconstruction principles.
Reconstruction-key	A distributed collection of analog-state conditions, synchronization relationships, validation states, replay-domain participation conditions, and governance mechanisms whose coordinated interaction enables authorized reconstruction.
Replay domain	A separately maintained operational condition that participates in synchronized replay interaction, such as waveform, timing, synchronization, transport, authorization, validation, or governance state.
Replay compatibility	An operational condition in which replay domains satisfy coordination criteria sufficient to permit synchronized replay interaction within replay-isolated reconstruction hardware.
Replay-isolated hardware	A hardware-confined reconstruction environment separated from generalized software-processing environments and persistent replay-state storage pathways.
Anti-stabilization	Hardware-governed behavior that inhibits formation or persistence of replay compatibility outside authorized synchronized replay participation.
Incompatibility propagation	System-level behavior in which divergence in one replay-domain relationship affects other timing, synchronization, validation, routing, waveform, or authorization relationships.
Topology mutation	Reassignment or reconfiguration of replay pathways, synchronization responsibilities, waveform roles, replay-buffer responsibilities, transport pathways, or authorization relationships.
Replay collapse	Physical or operational modification of replay conditions so that residual replay-domain fragments cannot readily reattach into a stable compatible reconstruction state.