6.1 Problem Statement

Return to Specific Requirements on Proposals

Mission-critical environments depend on structured information artifacts to coordinate operations across distributed organizations, platforms, and missions.

In defense and security contexts, as well as in other high-assurance domains, logistics, readiness, and sustainment functions depend on authoritative structured artifacts whose fields define requests, obligations, allocations, and status assertions. These artifacts determine how resources are assigned, actions are authorized, assets are tracked, and operational capability is assessed.

The data collected, the identification and definition of form fields, the structural constraints governing those fields, the semantic meaning assigned to them, and the interpretation logic applied to their values directly influence readiness assessments, resource allocation decisions, compliance determinations, and mission execution.

Historically, these artifacts were instantiated as paper forms. The structure of each form constrained what data could be recorded by defining specific fields, their organization, and permitted responses. Through these fields, resources were requested, actions were authorized, assets were tracked, and operational capability was assessed. The physical layout of the form embodied structural organization, while established doctrine and policy provided the semantic meaning for each field. Trained personnel interpreted reported values by applying governing rules within the context of established authority.

Most authoritative forms have transitioned from paper to electronic systems. Digital systems encoded form structures, implemented field identities and constraints within software, formalized the semantic meaning associated with form elements in data models and vocabularies, and partially or fully automated interpretation logic that trained personnel previously performed by applying doctrine and policy.

This transition produced significant benefits. Automation increased speed, consistency, scalability, and operational reach. Digital systems enabled real-time reporting, distributed coordination, and integration across platforms and jurisdictions.

However, these advances often resulted in islands of automation. Individual systems optimized internal workflows, yet interoperability across organizational, jurisdictional, and security boundaries remained loosely coordinated. Federation frequently relied on negotiated mappings, ad hoc integration mechanisms, and continued human intervention at system boundaries.

Structural definitions, semantic meaning, and interpretation logic became embedded within implementation environments. In many cases, operational data flow and governance control mechanisms became inseparable within the same implementation context. This coupling reduced the ability to manage structural and semantic evolution independently of deployed processing systems.

As a result, changes to data collection requirements, field definitions, semantic vocabularies, or interpretation rules often propagate unevenly across systems. Lifecycle management becomes complex, and interpretive authority becomes difficult to trace, reproduce, or transition across acquisition baselines. Reproducible interpretation under defined version conditions depends on specific system implementations rather than on architectural constructs.

Defense systems and other mission-critical environments operate across jurisdictional and security boundaries, including service authorities, coalition partners, sovereign nations, and compartmentalised classification domains. Each jurisdiction may maintain distinct structural definitions, semantic vocabularies, policy constraints, and interpretive rules. Operational effectiveness requires interoperability without surrender of structural or interpretive sovereignty.

Existing OMG specifications within the C4I domain address information exchange, interoperability, and semantic federation. However, no current specification defines a platform-independent Reference Architecture that governs the explicit separation and lifecycle control of data, structure, semantics, and interpretation across acquisition, jurisdictional, and security boundaries.

Despite differences in mission, jurisdiction, and domain, these environments share recurring structural patterns. Authoritative forms define structured data elements. Structured data elements are associated with governed semantic meaning. Semantic meaning informs interpretation logic. Interpretation logic produces operational outcomes.

These recurring patterns can be abstracted and formalized within a platform-independent Reference Architecture. Such abstraction reduces reliance on bespoke, tightly coupled implementations and enables modular composition of structural, semantic, and interpretive components. It also supports acquisition strategies that procure architectural roles and interface responsibilities rather than monolithic, tightly integrated systems.

A Reference Architecture supports coordinated acquisition strategies, simplifies system maintenance, enables clearer allocation of human and automated responsibilities, and improves traceability of authoritative decisions across lifecycle transitions.

Without architectural abstraction, systems evolve as isolated implementations. With architectural abstraction, mission-critical environments gain structural consistency, controlled variation, and modular adaptability across jurisdictions and security domains.

Modern mission-critical environments require more than digitised workflows and federated interoperability. They require governed architectural separation of data, structure, semantics, and interpretation, with an explicit distinction between operational processing flows and governance control mechanisms that manage structural and semantic evolution.

Such separation supports lifecycle stability, jurisdictional sovereignty, secure modular integration, and long-term reproducibility of interpretive outcomes.
