

# Feasibility Study for Design, Specification and Verification of MILS CORBA Middleware Running on a MILS RTOS

Jim Alves-Foss

Paul Oman

Carol Taylor

# Contractual Deliverables

- 2.5.1 Threat analysis for MILS RT-CORBA running on a certified MILS RTOS
- 2.5.2 Assistance to OIS in the development of a draft specification of MILS-CORBA.
- 2.5.3 Report on impact of OO techniques used by CORBA standards on design and verification efforts.
- 2.5.4 Assistance to OIS in the development of a Common Criteria Protection Profile for MILS RT-CORBA running on a certified MILS RTOS. This document will be referred to as PP-MRTC.

# Contractual Tasks

- **Phase 1 Tasks.** This phase focuses on the specification of the MILS-CORBA subset to be used in the development of the process documents in Phase 2 and the implementation in Phase 3.
  - 3.1.1 Review existing CORBA Documents including the following specific documents: Minimum CORBA, RT-CORBA, Fault-Tolerant, Online Update, Extensible Transport, Dynamic Scheduling, Load Balancing, Ada mapping and C++ mapping. This review will result in an understanding of the necessary features of a minimal CORBA kernel that will satisfy the security needs for a MILS system.
  - 3.1.2 Support OIS in the development minimal subset of CORBA required to provide support to develop complete implementations of MILS RT-CORBA, MILS FT-CORBA running on a MILS RTOS; this subset will be called MILS-CORBA. This subset will satisfy the security needs of a MILS system and will provide sufficient functionality to allow higher level components to implement the large subsets of CORBA.
    - **Deliverable:** Assistance with draft specification of MILS-CORBA; (report 2.5.2)

# Contractual Tasks con't

- 3.1.3 Conduct threat analysis for MILS-CORBA. This analysis will involve the types of threats typically found in a protection profile.
  - **Deliverable:** Report documenting threat analysis in a form useable in the development of a protection profile; (report 2.5.1)
- 3.1.4 Work with OIS to document the use of MILS-CORBA to implement the 3.1.1 features. This task generates a companion document(s) to the MILS-CORBA specification that demonstrate how MILS CORBA can be safely extracted from specifications such as RT-CORBA and Fault-Tolerant CORBA to allow a hierarchical implementation.
  - **Deliverable:** Reports detailing mapping of MILS-CORBA to CORBA documents
- 3.1.5 Evaluate feasibility of EAL7 certification for MILS-CORBA.
  - **Deliverables:** Report on impact of OO-techniques used in CORBA on the EAL certification; (report 2.5.3). Report on estimated complexity of MILS-CORBA.
- 3.1.6 Support OIS in development of Protection Profile for MILS-CORBA: PP-MRTC
  - **Deliverable:** Draft protection profile; (report 2.5.4)