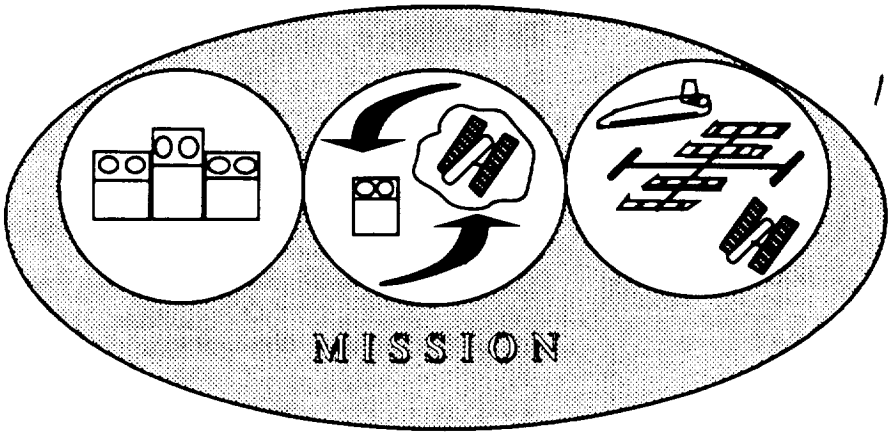


MISsion and Safety CrItical SuppOrt eNvironment

Executive Overview

by:

Dr. Charles McKay Dr. Colin Atkinson

Motivation and Goals

MISSION is concerned with MASC (Mission And Safety Critical) Systems which are :

• Large • Complex • Non-stop • Distributed • Real-time

For this kind of MASC system, there is a need to :

- improve definition, evolution and sustenance techniques,
- lower development and maintenance costs,
- support safe, timely and affordable system modifications,
- support fault tolerance and survivability.

The goal of the MISSION project is to :

"lay the foundation for a new generation of integrated systems software providing a unified infrastructure for MASC applications and systems"

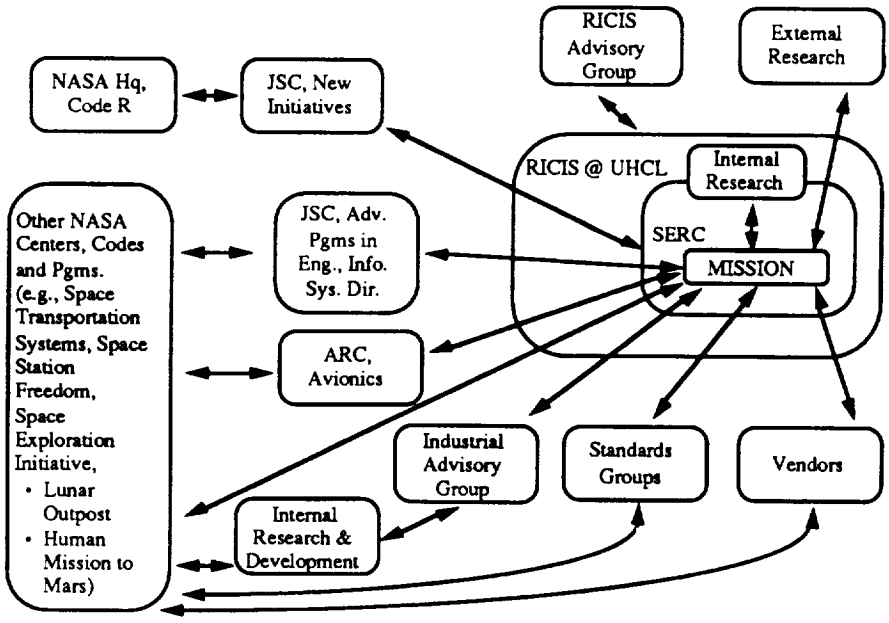
This will involve the definition of :

- a common, modular target architecture.
- a supporting infrastructure.

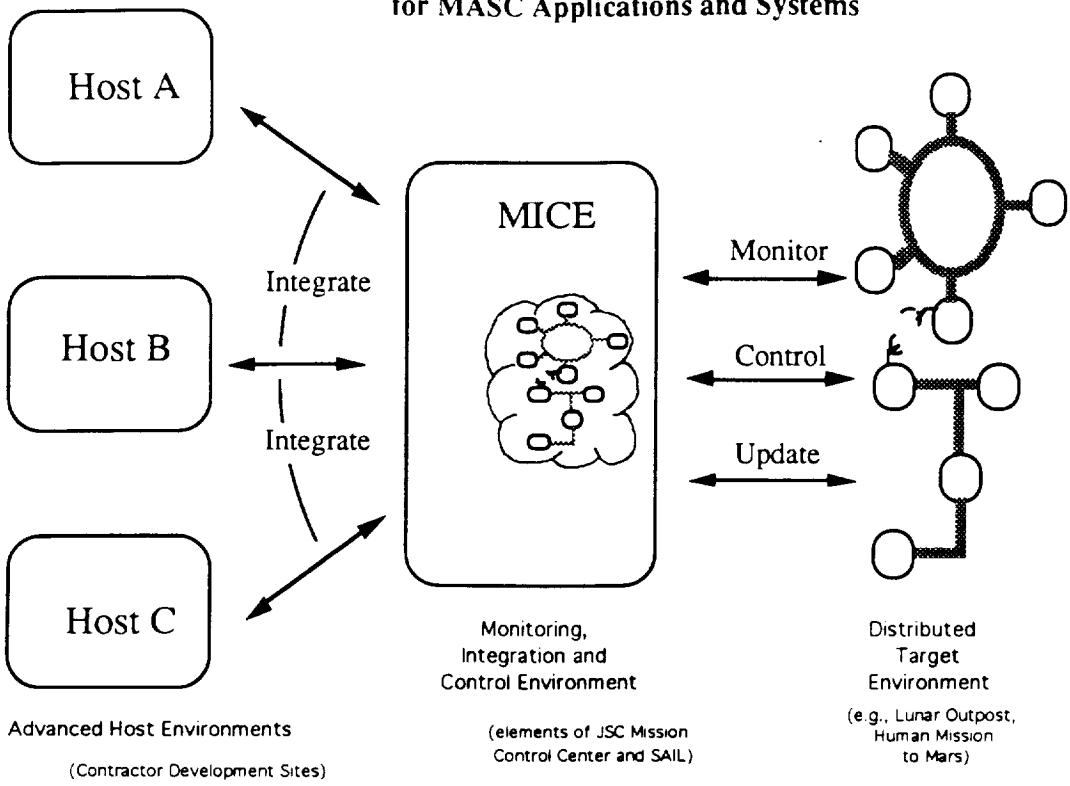
Background

SIZE	21 man years
DURATION	1990 .. 1996
SPONSOR	NASA Headquarters, Code R (through RICIS)
ADVISORS	Industrial Advisory Group (IAG)
Co PI's	Dr. C.W. McKay & Dr. C. Atkinson
PAST CONTRIBUTORS	• University of Bradford (Dr. Alan Burns) • Softech • GHG Corporation • Honeywell (Minneapolis) • Softlab (Munich)

MISSION Interaction Diagram



Integrated Life-Cycle Support Environment for MASC Applications and Systems

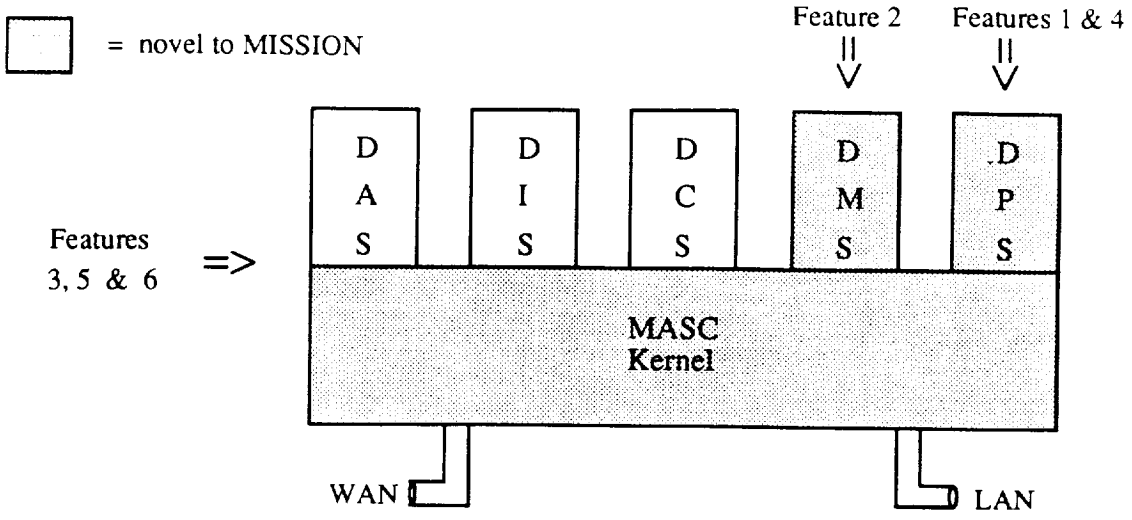


Requirements versus Features Matrix

	Fault-tolerant	Maintainable	Distributed	Survivable	Non-stop	Reliable	Target Features
1	•	•	•	•	•	•	On-board software models for monitoring and control
2	•			•			Dedicated software for system level fault tolerance and survivability
3		•			•	•	Separation of policies and mechanisms
4	•	•		•	•		Adaptable run-time policies during non-stop operation
5		•	•		•		Use of a full, concurrent object-oriented, paradigm
6	•			•		•	Firewalling of application and system objects
7						•	Multiple and adjustable levels of security and integrity
8			•				Synchronous and asynchronous communication mechanisms
9	•			•			Distributed nested transactions
10	•		•				Unique identification of all network messages
11	•			•			Redundancy management
12	•			•			Stable storage support for recovery

System Goals

Generic System Architecture (GSA) for the Distributed Target Environment (DTE)



DAS	Distributed Application System	MASC	Mission And Safety Critical
DIS	Distributed Information System	LAN	Local Area Network
DCS	Distributed Communications System	WAN	Wide Area Network
DMS	Distributed Monitoring System		
DPS	Distributed Policy System		

GSA Requirements on Supporting Infrastructure

Monitoring, Integration and Control Environment (MICE)

- Maintenance of precise models which describe the DTE :-

  software,
  hardware ,
  communications links,
  human-machine interfaces ,
  interactions with the environment.

- Distributed Command Interpreter
- Symbolic Diagnostic System

Advanced Host Environment (AHE)

- Construction of precise models of the DTE components
- Rigorous life-cycle approach to evolution and sustenance
- Precise software process models
- Support for special tools and modeling representations.

MISSION's Contribution

Distributed Target Environment

- GSA Requirements,
- GSA Interface Specifications,
- Guidelines for Applying, Tailoring, Modifying and Extending GSA,
- Proof-of-Concept Prototypes of Key and Unique Features.

Monitoring, Integration and Control Environment

- Form of semantic models,
- Guidelines for utilizing semantic models in MICE and DTE,
- Distributed Command Interpreter (DCI) interface.

Advanced Host Environment

- Process Model,
- Model-based life-cycle activities (CLAR/CLAD/CLAIM),
- Prototype semantic model repositories (LMS/OMS).

Anticipated Benefits

Improvements in :

Safety

- fault tolerance
- survivability (availability)
- risk management / certification

Adaptability

- upgrade interoperability
- dynamic reconfiguration

Cost Effectiveness

- reuse
- maintainability
- extensibility

Anticipated Application

NASA Future Programs

- Lunar Outpost
- Manned Mission to Mars

Upgrade to Current NASA Programs

- Space Shuttle
- Space Station

Other MASC Application Areas

- Avionics Systems
- Integrated Weapons Control Systems
- Industrial Process Control
- Transportation Systems
- Hospital Monitoring Systems

Schedule Overview

Significant accomplishments:

- Established MISSION test bed
- Defined semantic modeling representations in Ada-IRDS
- Prototyped Object and Library Management Systems
- Produced distributed nested transactions simulation
- Participated in relevant international standards groups

Future Milestones:

FY93

Begin second iteration of key components of the GSA

Specify interface sets for first iteration of GSA study (with simplifying assumptions)

FY94

Specify interface sets for second iteration of GSA study (without simplifying assumptions)

Begin second iteration of study of key infrastructure components

FY95/96

Complete proof-of-concept prototypes of key and unique features of the GSA

Complete specifications of the key infrastructure components