GRANT
IN-61-CR
1571

PORTABLE COMMON EXECUTION ENVIRONMENT (PCEE) PROJECT REVIEW

P23

Peer Review Final Report

C. Douglass Locke, Chairman
IBM Corporation

(NASA-CR-188016) PORTABLE COMMON EXECUTION ENVIRONMENT (PCEE) PROJECT REVIEW: PEER REVIEW Final Report (Houston Univ.) 23 p CSCL 09B
N91-22731
Unclas
G3/61 0001571

March 8, 1991

Cooperative Agreement NCC 9-16
RICIS Program Office

NASA Johnson Space Center
Information Systems Directorate
Information Technology Division

Research Institute for Computing and Information Systems
University of Houston - Clear Lake

T·E·C·H·N·I·C·A·L R·E·P·O·R·T

The RICIS Concept

The University of Houston-Clear Lake established the Research Institute for Computing and Information systems in 1986 to encourage NASA Johnson Space Center and local industry to actively support research in the computing and information sciences. As part of this endeavor, UH-Clear Lake proposed a partnership with JSC to jointly define and manage an integrated program of research in advanced data processing technology needed for JSC's main missions, including administrative, engineering and science responsibilities. JSC agreed and entered into a three-year cooperative agreement with UH-Clear Lake beginning in May, 1986, to jointly plan and execute such research through RICIS. Additionally, under Cooperative Agreement NCC 9-16, computing and educational facilities are shared by the two institutions to conduct the research.

The mission of RICIS is to conduct, coordinate and disseminate research on computing and information systems among researchers, sponsors and users from UH-Clear Lake, NASA/JSC, and other research organizations. Within UH-Clear Lake, the mission is being implemented through interdisciplinary involvement of faculty and students from each of the four schools: Business, Education, Human Sciences and Humanities, and Natural and Applied Sciences.

Other research organizations are involved via the "gateway" concept. UH-Clear Lake establishes relationships with other universities and research organizations, having common research interests, to provide additional sources of expertise to conduct needed research.

A major role of RICIS is to find the best match of sponsors, researchers and research objectives to advance knowledge in the computing and information sciences. Working jointly with NASA/JSC, RICIS advises on research needs, recommends principals for conducting the research, provides technical and administrative support to coordinate the research, and integrates technical results into the cooperative goals of UH-Clear Lake and NASA/JSC.

PORTABLE COMMON EXECUTION ENVIRONMENT (PCEE) PROJECT REVIEW

Peer Review Final Report

PREFACE

This report documents the findings of a review of a NASA-sponsored research activity, the "Portable Common Execution Environment (PCEE) Project". This review was requested by Mr. Paul Hunter, Information Sciences & Human Factors Division, NASA Headquarters. The Research Institute for Computing & Information Systems (RICIS) was asked to organize and host this review by Mr. Ernest M. Fridge, Deputy Chief, Software Technology Branch, Information Technology Division, Information Systems Directorate, NASA/JSC. The RICIS Program Office agreed to this request and contributed the required funding to conduct the review. Funds were made available from an account reserved for funding reviews of RICIS sponsored research. The review was held on February 14-15, at UH-Clear Lake.

The PCEE project is a RICIS activity sponsored by Code R of NASA Headquarters. The JSC technical monitor for this activity is Ernie Fridge. The project is directed by Dr. Charles McKay, Director of the Software Engineering Research Center of RICIS at UH-Clear Lake. The research team includes personnel from UH-Clear Lake, SofTech, GHG Corporation and Honeywell.

The purpose of the review was to conduct an independent, in-depth analysis of the PCEE project and to provide the results to the NASA PCEE project team. The review team was selected to represent a broad range of industrial experience in real-time systems, run-time environments and Ada. Importantly, NASA civil servants, UH-Clear Lake faculty and other RICIS researchers were purposely excluded from the team's membership to further ensure an outside, independent assessment.

The review team was tasked with evaluating the potential contribution of the PCEE project to the improvement of the life cycle support of mission and safety critical (MASC) computing components for large, complex, non-stop, distributed systems similar to those planned for such NASA programs as the space station, lunar outpost and manned missions to Mars. Two deliverables were requested: first, a presentation on February 15, 1991, summarizing their findings; and second, a written report covering the information in the presentation and additional recommendations concerning the PCEE project that the team deemed important or beneficial. This document includes the second deliverable.

RICIS has found the peer review process to be a very effective tool. It provides a project with an independent assessment of the effort, typically providing new insights that result in improved focus, increased efficiencies, enhanced understanding or better approaches to particular problems. It also provides a credibility check for management. Just having the project members get their thoughts together in preparation for such a review is rewarding to the project. Properly used and appreciated, peer reviews can save time and money in the long run.

Special thanks go to the members of the PCEE Review Team for their efforts in understanding, and providing constructive recommendations to, the PCEE Project Team. Within RICIS, thanks also go to Dr. Ted Leibfried, Director of RICIS Systems Research, for hosting the review, and to Mrs. Resa Ott of the Software Engineering Professional Education Center for professional and efficient handling of local arrangements.

A. Glen Houston
Director, RICIS

PCEE Review Team

February 14-15, 1991

Dr. C. Douglass Locke, Chairman
IBM Corporation
6600 Rockledge Dr.
Bethesda, MD 20817
(301) 493-1496

Dr. Ira Forman
Microelectronics and Computer Technology Corporation
3500 West Balcones Drive
Austin, TX 78759
(512) 338-3360

Mr. Enrique Gomez
IBM Corporation
3700 Bay Area Blvd.
MC: 6402B
Houston, TX 77058
(713) 282-8743

Mr. Duane Hybertson
Lockheed
1150 Gemini
Houston, TX 77058
(713) 282-6254

Mr. Kyle Rone
IBM Corporation
3700 Bay Area Blvd.
Houston, TX 77058
(713) 282-8399

Mr. Bill Selfridge
Rockwell International
12214 Lakewood Blvd.
MC: FB72, Bldg. 6
Downey, CA 90241
(213) 922-2935

Dr. David Weisman
Unisys
600 Gemini, Mail Stop U01B
Houston, TX 77058
(713) 282-4355

PCEE Project Team

February 14-15, 1991

Dr. Charles McKay, Project Director
Director, Software Engineering Research Center
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3830

Mr. David Auty
SofTech Houston Operations
1300 Hercules Drive
Suite 105
Houston, TX 77058
(713) 480-1994

Mr. Charlie Randall
GHG Corporation
1300 Hercules Drive
Suite 111
Houston, TX 77058
(713) 480-1994

Rakesk Jha
Honeywell Systems Research Center
3660 Technology Drive
Minneapolis, MN 55418
(612) 782-7320

Alan Burns
University of York
Heslington, York
Y015DD
ArpaNET: Burn@Minster.York.AC.UK

Karen Gunter
Technical Coordinator
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3833

PCEE Project Team
February 14-15, 1991

Mike Weisskopf
Lab Supervisor
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3833

Paul Brown
Program Analyst
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3836

Makhan Singh Matharu
Student Research Assistant
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3836

Vyankatesh Shanbhag
Student Research Assistant
University of Houston-Clear Lake
Box 447
Houston, TX 77058
(713) 283-3836

Peer Review Team Agenda

PORTABLE COMMON EXECUTION ENVIRONMENT REVIEW

February 13-15, 1991

February 13, Wednesday	Arrive at Nassau Bay Hilton
5:30 p.m.	Reception at Hilton with Team Members and NASA and University Participants
6:30 p.m.	Working Dinner for Team Members
February 14, Thursday	
8:00 a.m.	Shuttle from Hilton to UHCL
8:30 - 8:45 a.m.	Welcome and Logistics: Ted Leibfried, UHCL
8:45 - 9:00 a.m.	Introduction: Ernie Fridge, NASA
8:45 - 10:30 a.m.	Presentation
10:30 - 10:45 a.m.	Break
10:45 -12:00 p.m.	Presentation
12:00 - 1:00 p.m.	Lunch, Forest Room
1:00 - 2:00 p.m.	Executive Session - Team Members Only
2:00 - 2:15 p.m.	Break
2:15 - 4:15 p.m.	Presentation
4:15 - 4:30 p.m.	Summary
4:30 - 5:00 p.m.	Executive Session - Team Members Only
5:00 p.m.	Shuttle from UHCL to Hilton
6:30 p.m.	Working Dinner for Team Members
February 15, Friday	
8:00 a.m.	Shuttle from Hilton to UHCL
8:30 - 9:30 p.m.	Final PCEE Presentation
9:30 - 9:45 p.m.	Break
9:45 - 11:30 a.m.	Executive Session - Team Members Only
11:30 - 12:00 p.m.	Review Team Presentation
12:00 - 1:00 p.m.	Lunch, Forest Room
1:00 p.m.	Shuttle from UHCL to Hilton

International Business Machines Corporation

6600 Rockledge Drive
Bethesda, MD 20817

RECEIVED
MAR 1 1991
RICIS

March 8, 1991

Dr. Glen Houston
University of Houston - Clear Lake
Research Institute for Computer and
Information Science
P. O. Box 444
2700 Bay Area Boulevard
Houston, Texas 77058

Dear Dr. Houston:

The enclosed is the final report of the PCEE review team you requested. I believe we reached consensus on these findings and the recommendations, and we hope you will find this effort to have been helpful. On behalf of the team, I would like to thank you for your hospitality and support. Please feel free to contact me if you have any questions on the report.

Sincerely,

C. Douglass Locke

FINAL REPORT OF THE PORTABLE COMMON EXECUTION ENVIRONMENT (PCEE) PROJECT REVIEW TEAM

March 8, 1991

C. Douglass Locke, Chairman
IBM Corporation

Ira Forman
Microelectronics and Computer Technology Corporation

Enrique Gomez
IBM Corporation

Duane Hybertson
Lockheed Engineering & Sciences Company

Kyle Rone
IBM Corporation

Bill Selfridge
Rockwell International

David Weisman
Unisys

CONTENTS

Executive Summary

This report describes the findings of the PCEE Review Team formed by UHCL RICIS to assess the PCEE project. The following is a brief high-level summary of its findings. For a detailed description of the review, its findings, and its recommendations, see the attached report.

Following a 1.5 day review, the Review Team reached the following broad conclusions:

- The PCEE project was given high marks for its breadth of vision on the overall problem with Mission and Safety Critical (MASC) software. The PCEE project has formulated a sweeping set of objectives covering the entire life cycle of MASC software; the Review Team believes that such a vision is critical to eventual success in attacking this problem.
- Correlated with this sweeping vision, the Review Team is very skeptical that any research project can successfully attack such a broad range of problems. There is considerable concern that the PCEE project is attempting a solution to every component of the MASC software life cycle; the Review Team felt that it is highly unlikely that it can be successful, even if its funding were increased ten-fold.
- The Review Team makes several principal recommendations:
  - Identify the components of the broad solution envisioned, prioritizing them with respect to their impact and the likely ability of the PCEE project or others to attack them successfully, then re-plan the schedule relative to these priorities.
  - Rewrite its Concept Document differentiating the problem description, objectives, approach, and results so the project vision becomes accessible to others (such as NASA contractors, other researchers, etc.) The resulting document should undergo a peer review.
  - The Review Team feels that the MASC problem is of sufficient importance that NASA, in cooperation with other agencies with similar concerns (e.g., FAA) should undertake a much larger research effort, not only increasing PCEE funds, but also fostering and encouraging efforts by complementary and competing research teams. Increasing PCEE funds should be contingent on satisfactorily addressing the Review Team's other concerns (see the full report for details).

1.0 Introduction

This report describes the findings of a Review Team which was formed at the request of the University of Houston at Clear Lake's (UHCL) Research Institute for Computing and Information Systems (RICIS) to conduct an independent assessment of its Portable Common Execution Environment (PCEE) research project. PCEE is a major RICIS research project which is studying the critical problems involved in designing, building, and maintaining Mission and Safety Critical (MASC) software. Because of its obvious need for such systems, not only for existing projects such as the Space Shuttle and Space Station Freedom, but for future projects such as the Manned Mars mission, the principal funding source for the project is National Aeronautics and Space Administration.

Because of NASA's sponsorship of this project, the PCEE Review Team (PCEE/RT) members were drawn from NASA contractors and the Microelectronics and Computer Technology Corporation (MCC). The members of the Review Team were:

- C. Douglass Locke -- IBM -- Review Team Leader
- Ira Forman -- MCC
- Enrique Gomez -- IBM
- Duane Hybertson -- Lockheed
- Kyle Rone -- IBM
- Bill Selfridge -- Rockwell
- David Weisman -- Unisys

Prior to the review, the PCEE/RT received copies of a number of PCEE documents which allowed the PCEE/RT members to begin with a basic understanding of the general PCEE concepts and plans. At the review itself, members of the PCEE project team presented a detailed description of each of the components of the project, answering questions from the PCEE/RT. Following these presentations, the Review Team attempted to carefully consider each facet of the project, forming a number of conclusions in several areas.

UHCL provided an initial set of questions to the PCEE/RT prior to its inception; the PCEE/RT considered these questions, but did not necessarily consider this list to constitute a tight bound on its inquiry. It is the intent of the PCEE/RT that this report contains its findings related to all of these initial questions, as well as additional conclusions generated during the review.

In the remainder of this report, Section 2.0 describes our technical assessment of the PCEE research itself, including its goals, approach, and accomplishments to date. Section 3.0 describes the PCEE project's schedule and funding situation, as well as its ability to meet its schedule commitments, and Section 4.0 describes its deliverable outputs. Finally, Section 5.0 presents our recommendations, both for the PCEE project itself, and for its principal funding agency relative to its critical needs for solutions to the problems addressed by the PCEE project's objectives.

2.0 Assessment of PCEE Research

To assess the PCEE project as a whole, the PCEE/RT began with an assessment of its research topic, its goals, its approach to fulfilling these goals, and its current progress toward them.

2.1 Topic Significance

In the NASA environment, Mission and Safety Critical (MASC) software consists generally of large, long-lived, non-stop systems which must be maintained in place. MASC software shares the usual difficulties of other large, complex software projects (such as commercial operating systems), but operates in an environment in which errors or failures can result in loss of life or property; MASC software cannot operate with the same correctness (either logical and temporal) properties as other systems. The PCEE project objectives constitute nothing less than a redefinition of the entire software life cycle of MASC software, creation of a development model, procedures, a production environment, an execution environment, and a maintenance environment.

Thus, the success of the PCEE Project would have a significant impact on the Mission and Safety Critical (MASC) software systems that are essential to the success of NASA. The high cost of failure of these systems is further amplified by their high national and international profiles (e.g., Shuttle, Space Station Freedom). In addition, the PCEE problem definition subsumes almost all of the significant problems that arise in major aerospace applications (e.g., air traffic control); a breakthrough in the ability to produce MASC systems by the PCEE Project would produce spin-offs that would be of great value in many environments. Thus, if the PCEE Project succeeds in providing an approach to managing the increased complexity of these systems, ensuring mission success and safety, then the cost of this research becomes insignificant.

2.2 Research Goals

The PCEE Project team has accepted all of these challenges. The PCEE/RT strongly commends the project team for its breadth of vision, covering virtually all aspects of MASC software efforts. This broad outlook clearly envisions MASC software which encompasses almost all of the characteristics of the most complex systems being considered today; the issues which are addressed by the PCEE team include safety, security, real-time response, distribution, fault-tolerance, portability, maintainability, and reconfigurability. PCEE envisions the management of such systems through the successful completion of the following five activities:

1. Develop a life-cycle model for the construction, maintenance and evolution of MASC components

2. Develop separate environments for 1) development, 2) integration, deployment, monitoring, change control, and maintenance, and 3) execution of MASC components

3. Specify a comprehensive design methodology for building MASC components

4. Develop prototype tools to support this aforementioned methodology

5. Contribute to the evolution of policies, standards, and guidelines for MASC components

The PCEE/RT feels that the PCEE Project goals need not be as ambitious as those proposed in the PCEE Concept Document to be of great value to NASA. There is considerable concern within the PCEE/RT that maintaining such a wide range of goals for a single project will result in inevitable trade-offs among these goals which could easily keep the project from fully achieving any of its goals.

2.3 Research Approach

A fundamental tenet held within the PCEE Project is that the entire software life cycle must be addressed in order to ensure the that MASC software components can be constructed which can meet its requirements. This assertion results in two methodology design decisions which drive the PCEE research approach. The first of these decisions is that the overall MASC environment should be divided into three individual environments: 1) the host environment, 2) the integration environment, and 3) the target environment. The PCEE/RT found the reasons for defining three (rather than the usual two) such environments to be compelling. The second methodology design decision is that MASC software should first be designed only to meet its functional requirements, then subsequently transformed by specialists to exhibit additional properties (such as real-time response, fault tolerance, distribution, security, etc.). The PCEE/RT found the arguments for this second decision to be considerably less compelling. While the ability to separate functional properties from other properties is clearly desirable, the PCEE/RT was not convinced that it is possible for practical systems.

The PCEE Project team approach includes prototypes of all three environments, including all the ancillary tools. Prototyping is an excellent method to gain and communicate this understanding. Certainly prototyping the target environment will be absolutely necessary; prototyping the other environments is desirable. Furthermore, an understanding of the target environment (obtained through prototyping) is necessary to derive the requirements for the two other supporting environments. This observation leads one to conclude that although a preliminary design of the entire MASC software environment based on PCEE methodological considerations is a commendable idea, in the light of limited resources, prototyping should concentrate on the target environment before addressing the other two environments.

2.4 Progress toward PCEE Research Goals

The PCEE/RT believes that the progress made in FY '90 serves as a solid foundation for a significant future research contribution. The PCEE project team has conducted research in the following areas:

1. The prototyping of coarse-grained Ada components for two processor types.
2. The demonstration of command and monitoring interactions between the target and integration environments.

This work is consistent with the PCEE/RT's and the PCEE project team's belief that the target environment determines the requirements for the other two environments.

The PCEE project team has an established set of goals and schedules that does not leave time to specify one subject area before moving on to the next. For example, solutions to all three of the following are included in the PCEE project's research goals for its investigation:

1. The methods of partitioning Ada programs to execute in a parallel and distributed configuration,
2. The ability to test the execution of those programs in that configuration, and
3. The services required for the processor kernel to permit independence of the hardware platform

At present, the PCEE project is approaching these investigations by constructing prototype environments which could be used to build MASC software. The PCEE/RT believes that this approach is not likely to be successful in the light of the desired schedule and available resources.

3.0 PCEE Schedule and Funding Assessments:

Schedules and detailed milestones for the next six years were defined and presented to the review team. The PCEE/RT considered it commendable that the PCEE team has established a road map for their project that extends well beyond the research stage into a final prototype, a near production system. This enforces and demonstrates the clear vision and commitment that will be extremely beneficial to the project. However, given the current, and even any reasonable increases in funding, the PCEE/RT finds the schedules to be extremely aggressive. The PCEE/RT believes that a much higher level of funding and skills would be required to deliver the even a sizable portion of the products defined in the schedules as stated by the PCEE team.

A number of factors were considered for this assessment:

- **Scheduled deliverables (Requirements)** - The deliverables described in the six year plan include methodologies, concept documents, tools, prototypes, new techniques

and solutions to many difficult problems, standards, and a test bed. This is further complicated by the fact that the PCEE approach attempts to address host, integration, and target environment issues.

- **Available funding as presented by the PCEE team** - Four proposed levels of funding were presented to the review team. The current level is $475,000, although the PCEE project team established a minimum level of $632,000 for its base set of deliverables. The schedules presented assumed this minimum level of funding rather than the current lower level. Additional funding would result in additional deliverables according to the PCEE team.

- **Other dependencies** - The PCEE research is dependent on progress in a number of related research and development efforts:

  - Language dependencies (e.g., Ada 9X) and real-time systems challenges.
  - Required hardware and software
  - State of the software and hardware technology
    - Distributed systems technology still evolving
    - New hardware architectures being developed
    - Programming techniques still evolving

Our assessment, then, is that the schedules are unrealistic.

With respect to the PCEE research objectives and its extremely aggressive schedules, the funding presented is certainly insufficient to cover the work described in the review. In fact the work described is so broad in scope that the PCEE/RT believes the deliverables described cannot be produced in anything close to the effort allotted.

As a partial rationale for the PCEE/RT's determination of insufficient funding consider that the work described is similar to the Phase A and B studies of the large complex support system defined as the Software Support Environment (SSE) of the Space Station Freedom project. There are a number of points of similarity between the two types of work:

- High level architecture
- Portability layer
- Distributed system
- SPF, integration environment
- Tools, rules, policies
- Target architecture studies

The software support environment portion of the work described for PCEE is actually larger than this because of the inclusion of the portability layer of the target and the

inclusion of a command and control center (i.e., PCEE's Integration Environment). The estimated cost of such an environment for the Space Station is $140-150M for the full scale development. Phases A and B would be approximately 20% of that so the estimated cost of these studies would be $28-30M. PCEE would, of course, be larger than that since it contains more work.

The principal PCEE/RT conclusion from this is that an expenditure of $3.5M, the currently planned total budget, will not support the work described. Increasing the funding to $10.5M will still not solve the problem as that is still not sufficient to cover the effort described in the current schedules.

4.0 Assessment of PCEE Deliverables

There was a long list of deliverables that was presented to the PCEE/RT, including:

- Testbed
- Host Environment:
  - Environment Framework
  - Eight Tools/Toolsets
  - Standards, policies, practices, guidelines, and procedures
  - (Ancillary) Reusable software components
- Integration Environment:
  - Precise Semantic Models
  - Capability to monitor and control baselines in the target environment
  - Capability to support emergency interactions with target
- Target Environment:
  - Five system software interface sets for MASC components
  - Interface to mechanisms of a MASC kernel

Again, this list reflects what the PCEE/RT feels is the overly-ambitious nature of this project, particularly in the light of its schedules and available resources.

The primary deliverable available to the PCEE/RT for review was the PCEE Concept Document, dated January 24, 1991. This document described the approach to MASC systems proposed by the PCEE project team in some detail. The document contains a significant amount of information, but the PCEE/RT assessment of it parallels its analysis of the project as a whole: it tries to do too many things at once. The problem statement is not sufficiently explicated and consequently does not sufficiently motivate

the solution that is presented. The fundamental problem to be solved, its derived requirements, architecture, design, assumptions, and research areas are all intertwined throughout the document and are not clearly distinguished from one another.

Also conspicuously absent from the Concept Document is an enumeration of the unsolved research problems that must be overcome in order for the PCEE to come to fruition. Such a list would greatly aid in identifying research (and maybe even commercial products) that can be obtained elsewhere.

5.0 Review Team Recommendations

The PCEE/RT strongly feels that the importance and complexity of mission and safety critical (MASC) software for large, nonstop systems cannot be overstated. We agree with NASA that it is crucial for the issues associated with implementing and maintaining such systems to be clarified, to assure that approaches are developed which can minimize their inherent risk. As indicated above, no single project can possibly document and solve all MASC problems. However, the PCEE project has provided an important initial model that must be refined and validated to help clarify these MASC issues to provide a foundation for developing solutions.

In the light of this analysis, the PCEE/RT makes a number of recommendations about the overall focus, deliverables, funding and schedules. In all of these recommended changes, our recurrent theme is that the strengths of the PCEE team should be exploited: its understanding of the overall MASC problem and its vision for a comprehensive solution should be emphasized over the production of prototype deliverables.

5.1 Overall Recommendation to NASA

While it seemed initially beyond the scope of the PCEE review, the PCEE/RT noted several factors resulting in recommendations that NASA should review (and probably significantly increase) its allocation of research resources to the problem of MASC systems development and maintenance. Projects both complementary to, and competitive with, PCEE should be initiated to address this broad subject and many of its components.

As a single example, the PCEE/RT notes that the PCEE project strongly bases its approach on the use of the Ada language because of its clear advantages relative to most of its competitors in producing safe software. Current research in distributed and parallel computation, however, is investigating languages with fundamentally different characteristics which make managing fine-grain parallelism more tractable; such approaches could significantly reduce NASA's long-term risk, especially if PCEE were to fail to provide the complete MASC solutions at which it aims.

In the light of the similar needs of other government agencies, NASA should also investigate possible additional inter-agency activities, such as FAA's Advanced Automation System. Multiple, complementary research projects offer far better opportunities for success; all research, including PCEE, contains risk, this risk is particularly present in projects with visions as broad as PCEE's. Such projects should include:

- The conceptual integration of diverse, known approaches to components of the MASC problem
- Proof-of-concept demonstrations
- Research into solutions to less well understood problems

5.2 PCEE Technical Recommendations

Our recommendations for PCEE include actions to clarify current work and to review and prioritize future work.

5.2.1 Generate List of Methods and Approaches

Given the breadth of the MASC problem, solutions must involve the integration of well-understood techniques with the results of cutting-edge research. The PCEE project should develop a list of methods and approaches that are part of the current PCEE vision for MASC systems implementation. Each method or approach should be annotated to indicate its status (e.g., "successfully implemented","documented in the literature", "understood but not well documented", or "requires research").

5.2.2 Clarify and Publish Current Results

During our review, it was suggested that the PCEE team has developed approaches which address several important problems. For example, one of these is the generation of precise models for MASC software components and the establishment of a context-sensitive recovery enforcement policy to avoid possibly inconsistent attempts at failure recovery. We feel that the PCEE team should document (via technical reports or papers) their understanding of each of these methods or approaches for which no other comprehensive reference is available. To facilitate understanding, the description of each approach should include illustrations of its application to non-trivial problems.

Specifically with reference to the PCEE Concept Document, the PCEE/RT believes that it requires a significant rewrite. As described in Section 4.0, it currently contains a mixture of problem understanding, requirements, lifecycle vision, design, and philosophy. While each of these views offers additional insight into the MASC problem, they should be clearly distinguished. Several volumes should be produced. First, there should be a clear statement of the problems of large, nonstop systems and

their implied MASC software requirements. Next, the current PCEE high-level perspective should be documented to provide the important full life cycle vision that has been developed. (This document should avoid low level details. However, it should clearly relate the vision back to requirements.) Low-level design decisions should be documented, and their relationship to the overall vision should be clarified. Finally, we would urge that a list of research topics which must be solved for PCEE to be successful be compiled and included in the revised Concept Document(s). The resulting document should undergo a formal peer review (see Section 5.2.5).

5.2.3 Improve Terminology

As these new documents are created, current PCEE terminology should be reviewed to assure that it supports understanding. Terms used by the PCEE project that have counter-intuitive meanings (e.g., an Integration Environment that includes Command and Control, or a DOS that includes policies, but not mechanisms) deter understanding. Terms carefully chosen to be consistent with common usage can assist in clarifying these inherently complex issues.

The overloading of technical terms (such as PCEE, which is used as a project name, an environment name, and a run-time structure) should be avoided unless the differences in meaning are easily inferred from context.

5.2.4 Separate and Prioritize Research Topics

The PCEE/RT has some concern about the apparent tight coupling of many research topics. It is important that issues be addressed separately to avoid interference among competing technologies and goals. To support decoupling, research topics identified in the overall list of methods and approaches should be prioritized. We are in no position to suggest the appropriate priorities, but we feel that the high-level task of clarifying and refining the overall PCEE MASC vision may provide the greatest benefit.

Once priorities have been established, a new project plan should be developed to address high priority issues first. Each issue should then be investigated under the *assumption* that the other problems have been solved. In this way, real progress can be made on some of the problems, prior to solving all the problems. The revised plan should also establish clear intent and identify mechanisms for ongoing, close connections to other researchers.

5.2.5 Increase and Formalize Communications and Feedback

Mechanisms need to be established to present and review PCEE approaches and reports, in a timely manner, with other researchers and the sponsor (NASA) community. The current, informal review process has suffered from the lack of continuity and commitment of those to whom the project has been presented. A more formal review process will not only address this problem, but it will also ensure meaningful feedback and will help retain an appropriate project focus. A Technical Advisory Group established through RICIS could provide the right mechanism.

5.2.6 Canonical Problem Definition

An important step in the solution of many critical research problems is the development of "Canonical" problems (e.g., the Dining Philosophers) which serve to define the essence of a difficult problem and provide a framework for describing solutions. Such a test case would significantly aid in ensuring that all project personnel are working to the same goals. In addition, a canonical test case would aide in communicating results within the team and to the consumers of the teams output. Canonical test cases are not easy to devise; but a great one (one that immediately conveys understanding of the problem and focuses world-wide research) would be worth the full PCEE budget.

5.2.7 Separation of Functional Design from Performance

The review committee has some reservations with respect to the design methodology proposed by the PCEE team providing for a domain expert to take a functionally correct software design and add performance (e.g., real-time, distribution, fault-tolerance) attributes afterward. The PCEE project team proposed that they will research this in the context of Ada and at a fine level of granularity. This is a very difficult problem; theoretical research in this area is proceeding with language concepts that are quite different from Ada. In the presence of inter-process (a.k.a., shared, global) variables, the problem of post-partitioning parallel threads in Ada and at a granularity lower than the task level is one that seems to require the maintenance and propagation of very complex context information. Rather than a fully general solution to this problem, the PCEE/RT would expect design and programming guidelines that avoid the trickier issues. This implies that the specialists (e.g., a distribution specialist, a fault-tolerance specialist, etc.) would be involved with the applications programmer during design (this is also in the spirit of Concurrent Engineering).

We recommend a more careful analysis of the impact and feasibility of the partitioning design decision on the overall PCEE research plan.

5.3 Funding

After such a brief review, it is difficult to make precise funding recommendations. In addition, it must be noted that the PCEE/RT did not do any analysis or audit of the PCEE financial management. However, based on the importance of the research objectives and the results to date, and assuming that the structural changes (e.g., deliverables, prioritization, additional senior staff) recommended can be successfully made, we believe that the PCEE project warrants a significantly increased commitment by NASA. A funding level of $1.5M per year can be justified easily from a technical perspective. This would allow the PCEE team to establish closer contact with other researchers and to clarify and report their results more broadly throughout NASA. It would also provide for the increased project resources described in the following section.

5.4 PCEE Resources

We feel that personnel resources should certainly be increased. In particular, we strongly suggest the addition of another senior staff member, preferably a UHCL faculty member, to provide additional leadership to the project. We do not believe that a project with the breadth of objectives and scope of PCEE can maintain its momentum and vision without close communication within the team at a senior staff level.

5.5 PCEE Deliverables

The review team feels that there has been undue emphasis on PCEE software deliverables. We recommend that the project be refocused on products such as technical reports and papers. Papers, especially, will produce the continuing dialog with the research community which is essential to maintain its integrity. Prototypes and proofs-of-concept should be delayed at least until the current state of the project is documented. This specific set of deliverables and their schedules should be clearly identified in the PCEE project plan.

The PCEE/RT believes that the objective of these investigations should be a sufficient understanding to prepare a specification of the requirements for actual MASC environment implementations, rather than the implementations themselves. Specifications thus produced would then be subjected to peer review as well as exploration of alternative design and implementation solutions to meet the specified requirements. This follow-on activity could be conducted by the PCEE Project team or by others, such as industrial IR&D programs.