NISTIR 5677

Center for High Integrity Software System Assurance -Initial Goals and Activities-

Dolores Wallace
Marvin Zelkowitz

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 5677

Center for High Integrity Software System Assurance -Initial Goals and Activities-

Dolores Wallace
Marvin Zelkowitz

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

June 1995

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arati Prabhakar, Director

Abstract

Software is a major factor in corporate operations, consumer goods, military systems, environmental and energy services, communications, health care, and government operations. High integrity software is software that can and must be trusted to work dependably and is a growing necessity for the ability of United States industries and government to function. To enable the U.S. software industry to build high integrity software and to provide U.S. industries and government confidence in the software systems on which they are dependent, NIST created the Center for High Integrity Software System Assurance (CHISSA) to establish criteria for software assurance for use by those who build or evaluate these systems. The measurements and associated methods will be embodied in a software development and assurance framework that will enable CHISSA to identify needed research in high integrity software assurance, to accelerate use of effective technology into industry, and to develop standards and guidelines in cooperation with industry, other Federal agencies, and the research community.

1 Introduction to CHISSA

High integrity software is software that can and must be trusted to work dependably; it is a necessity for the ability of United States industries and government to function [11]. To enable the U.S. software industry to build high integrity software and to provide U.S. industries and government confidence in the software systems on which they are dependent, NIST created the Center for High Integrity Software System Assurance (CHISSA) to establish criteria for software assurance for use by those who build these systems. Its purpose is to facilitate the development and use of solutions for assuring high integrity software systems to serve industry needs with respect to these systems. This report describes the initial goals for CHISSA and presents a preliminary description of the activities to be undertaken in the near term.

CHISSA was organized to enable industry to build high integrity software systems using technology whose benefits have been defined and *measured*. (This goal of "measured" will be explained shortly.) To achieve this goal, CHISSA has these objectives:

- collaborate with industry to determine high integrity software technology requirements,
- identify high leverage research topics and potentially beneficial research results,
- identify technology issues between software and other system components,
- provide a mechanism for linking research, measurement, and transfer of software technology related to similar efforts for other system components,
- provide for measurement and assessment of technology in real application projects,
- identify mechanisms for insertion of technology,
- promote continuing training for engineers and scientists,
- promote development of guidance and standards, and
- provide results that will be made available to those organizations developing rules, policies, or contracting requirements to help them ensure that those rules, policies, and requirements are economically and technically feasible.

1.1 CHISSA Interactions

CHISSA will set its own agenda, based upon interactions with many related groups (Figure 1). Key groups include:

- *HISSA*. The NIST High Integrity Software System Assurance (HISSA) program is currently involved in several high integrity software activities. This includes work performed as a result of contracts with other agencies, development of technical products in software engineering,

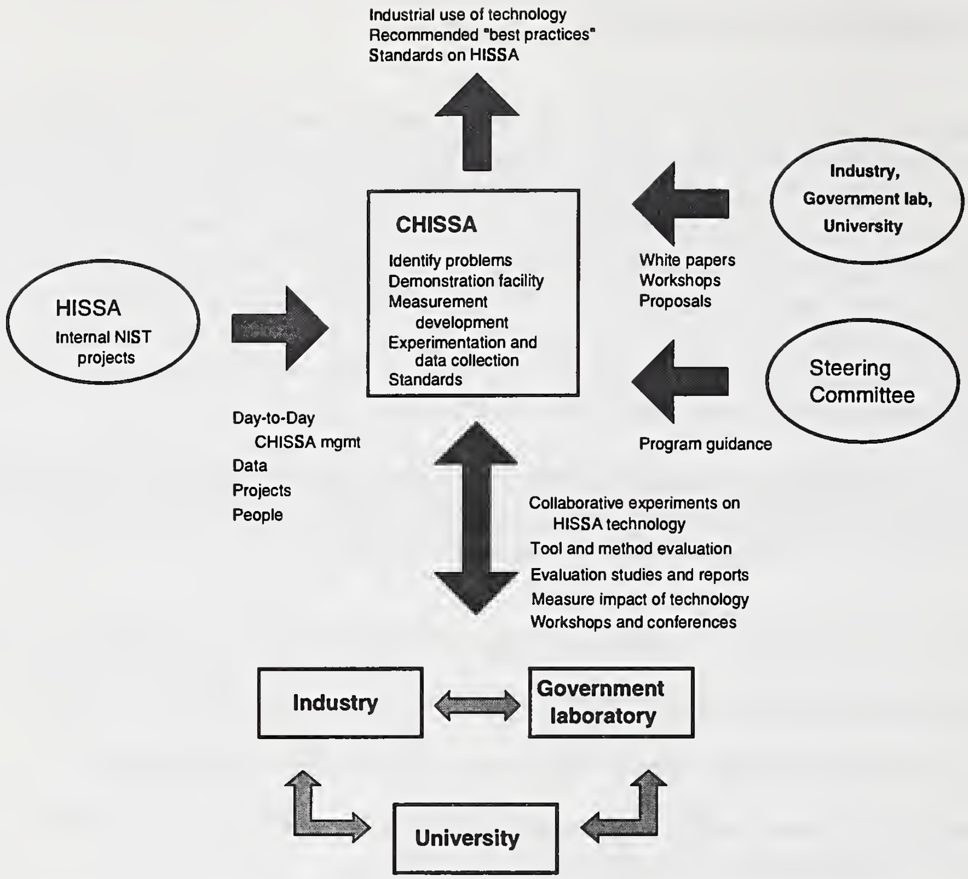

Figure 1: CHISSA interactions.

organization of the NIST High Integrity System Lecture series, organization of the annual COMPASS assurance conference, and other tasks in the high integrity area. HISSA personnel will provide day-to-day management of CHISSA activities, and various HISSA projects and their data will provide input to CHISSA processes.

- *Industrial, University, and Government Laboratories.* CHISSA will seek input from industry, other government laboratories, and universities on problems of mutual interest. Via a series of white papers, workshops, conferences, and proposals, the various communities will make their needs known to CHISSA. This is described more fully in Section 1.1.1.

- *Steering Committee.* An outside Steering Committee of industrial, government, and academic experts has been organized to provide an independent assessment of the role for CHISSA and for providing program guidance on CHISSA plans. The role of the Steering Committee is explained more fully in Section 1.1.2.

1.1.1 Role of industrial, government, and university input

CHISSA will operate in concert with the needs of industry. Via a series of calls for white papers, industry, government, and university experts can make their needs known to CHISSA. In late 1994 a call for white papers resulted in 94 submissions to CHISSA. These were reviewed and formed the basis for some of the early decisions described in this paper.

In the future, additional white papers will be requested. Also, various workshops and conferences will be organized for more interactive communication with industrial and academic leaders. This will provide the stimulus to ensure that CHISSA continues to address the needs of industry.

1.1.2 Role of Steering Committee

In October 1994 a Steering Committee was formed to help NIST establish CHISSA and to set its initial scope. This Steering Committee (given in Appendix A) consists of government, university, and industrial personnel who are experts in the field of high integrity software systems.

The Steering Committee reviewed all the white papers that were submitted as a result of the 1994 call for white papers and provided suggestions for developing an initial set of tasks for CHISSA to undertake. The Steering Committee will have a continuing role including activities such as assisting in refining CHISSA goals and objectives as they evolve over time, providing personnel for some high level tasks, and developing mechanisms for accelerating acceptance and use of technology. The Steering Committee may provide guidance on implementations of tasks to achieve CHISSA goals. Of course, they will help to identify acceptance criteria for CHISSA products and may provide reviews.

As CHISSA evolves, the Steering Committee may change or may be enlarged. CHISSA is intended to be evolutionary and will adapt to the needs of industry.

1.2 CHISSA Operations

As a result of the evaluation of the white papers and consultation with the Steering Committee, CHISSA's main function is to interact with various industrial, university, and government organizations in order to act as a facilitator in developing joint projects of interest to all. Most of this report describes these interactions.

The result of these collaborations will be a series of reports, measurements, data, experimental results, and tools that will be made available to the community at large via the World Wide Web (WWW), NIST reports, workshops, and published papers in journals and at conferences.

Early concerns

In order to understand the early goals for CHISSA, it is necessary to understand the climate under which CHISSA was formed. Funding from NIST is sufficient to support NIST coordination of CHISSA activities and for building some of the infrastructure, as described in this report. However, because the availability of funds for supporting needed research is limited, selected research, development, and testing will be supported as follows:

- *CRADA.* The Cooperative Research and Development Agreement (CRADA) is a contractual arrangement between NIST and commercial enterprises allowing for collaborative research and development and for shared use of NIST facilities. The CRADA carefully describes the legal implications and intellectual property rights of the industrial partners and government. CHISSA will provide focus for research organizations interested in working on specific problems with other companies and government agencies sharing those problems. CHISSA will act as a clearinghouse for reports to be shared among all participants, for data to be made available to the community, and for making tools available for others to evaluate.
- *Funding agencies.* CHISSA will work with other funding agencies (e.g., ARPA, NSF) in order to identify and propose programs that address mutual concerns in high integrity software.

CHISSA has funding for the remainder of fiscal year 1995 (through September 30) and anticipates funding for fiscal year 1996. Two Steering Committee meetings have been held. This planning report addresses CHISSA planning through May of 1995.

2 Fostering High Integrity Software Systems

CHISSA must first understand the mechanisms that provide for high integrity software system assurance and then accelerate the acceptance of those mechanisms within industry. At the April 11, 1995, CHISSA Steering Committee meeting several approaches toward addressing the development of high integrity software systems were identified and are explained in this report. CHISSA will be a catalyst for ensuring that academic researchers, industry, and the various funding agencies address these processes. The following subsections describe CHISSA actions and provide more detail about CHISSA objectives.

2.1 Industrial Needs

In order to provide a baseline of industry needs in the high-integrity arena, CHISSA issued an initial call for White Papers in late 1994. Ninety-four papers were submitted in response to this request. The papers were categorized as follows:

A. Infrastructure issues: These papers described attributes applicable to any technology that may be employed in solving industry needs. The infrastructure issues that were raised included:

1. *Experimental methodologies* need to be developed in order to determine the effectiveness of each new technology that is proposed as a potential solution.

2. *Standards* need to be investigated in order to permit multiple vendors to provide necessary services and products as solutions to industry needs.

3. *Educational opportunities*, both industrial training and university curricula, need to be developed as a means to increase general knowledge of such solutions.

4. *Technology transition* is a continuing problem as industry needs to learn about and adopt new techniques that will help solve its problems.

5. *CHISSA's role* was the subject of several of the white papers, which described mechanisms CHISSA could use to help industry produce high-integrity software.

B. Fundamental technologies: These papers describe core research areas that can be applied to multiple problems within CHISSA's domain. Sample technologies that were raised include:

1. *Formal methods* provide a precise notation and semantics for discussing attributes needed for high integrity software systems. These may be applied across multiple domains, such as specification models for precise specifications, security models for assurance concerns, verification models for system correctness, etc.

2. *Languages* provide the notation used in the translation of a specification into an executable object. This may provide the notation for specifications, executable source programs, security policies, communication protocols, etc.

3. *Measurement technology* is needed to provide feedback on the effectiveness of each evaluated technology. This is an important part of the experimental methodologies component of the infrastructure category.

4. *Theory* provides the basic models and metrics used by the other components of this category in determining the underpinnings of what constitutes a high integrity software system.

5. *Process* provides the basic mechanisms used to develop high integrity software systems. Process determines which technologies need to be applied to solve specific application problems.

C. Engineering technologies: These papers describe specific problems that industry is currently facing. Solutions to these problems are often applications of the previously mentioned fundamental technologies as built into specific computer tools or defined processes. Sample problems raised by the white papers include:

1. *Requirements analysis tools* are needed for proper development, understanding, and traceability of requirements and specifications.

2. *Design and analysis tools* are needed for reliable translation of requirements and specifications into executable programs.

3. *Validation and evaluation tools* are needed for determining the correctness and reliability of developed systems.

4. *Assurance mechanisms* are needed to validate architectural concerns such as security, fault tolerance, and safety of systems; system services and protocols; and human computer interfaces.

5. *Engineering management issues* need to understand legacy systems and the need for reuse, reengineering, and use of COTS (Commercial Off the Shelf) tools in the development of new high integrity software systems.

Appendix B provides additional information about the set of white papers.

CHISSA must address several large issues early if it is to have positive impact on industry. The white papers influenced early CHISSA priorities in terms of both short and long term goals.

2.2 Short Term Goals

From the white papers several messages came through very strongly:

- many U.S. industries are unaware of usable technology,
- many research experiments are not being conducted with appropriate analysis of the collected data,
- there is no current service providing guided access to information on software methods or industry needs, and
- research results are not packaged in a manner conducive to industry adopting the technology.

In order to remedy these fundamental infrastructure problems, CHISSA will address measurement and dissemination of information as crucial early tasks. Only after CHISSA develops the ability to measure the impact of high-integrity processes on system products and informs industry which processes are effective will it be able to investigate the particular technologies themselves. For example, it makes no sense to first study formal methods (1) if there is no scientific basis upon which to decide if the various technologies are effective, and (2) if effective, there is no mechanism to inform industry of that fact. Sadly, both of these conditions are true within the software development domain today.

> "We find it surprising that some standards mandate various techniques but either give no reason why they should be used or justify them with statements that are variations on 'Technique X is good and leads to better software.' For safety-critical applications, it is not sufficient to seek software that is *safer* or *more reliable* in an imprecise sense

> because that which is achieved might still be inadequate. With no precise definition of software safety, for example, it is not possible to state that a given software entity is safe. It is pointless to develop a standard that prescribes the use of various techniques for achieving something that is itself not defined." [5]

2.2.1 Measurement program

CHISSA's primary early goal is to address the role of measurement within software engineering. Software measurement is quite different from hardware measurement. Hardware components break over time, so concepts like Mean Time to Failure (MTTF) or Mean Time Between Failure (MTBF) make sense in the hardware domain in deciding on the reliability of a physical device. Data bandwidth over a communications line (e.g., megabits per second) also can be easily computed as a hardware performance measure.

There is no such analog for software. Much has been written about metrics for software development (e.g., function points, lines of code, cyclomatic complexity, software science); however, each of these only provides a rough estimate of the underlying measurement. Effective theories of measurement must still be developed.

> "Five questions should be (but rarely are) asked about any claim arising from software-engineering research:
>
> - Is it based on empirical evaluation and data?
> - Was the experiment designed correctly?
> - Is it based on a toy or a real situation?
> - Were the measurements used appropriate to the goals of the experiment?
> - Was the experiment run for a long enough time?
>
> ... Unfortunately, software methods and techniques often find their way into standards even when there is no reported empirical, quantitative evidence of their benefit. This is true of even the most sophisticated methods, developed with mathematical care and precision." [2]

Software process has been proposed as a way out of this dilemma. The concept behind this idea is simple: Since the ultimate property of interest cannot be measured (e.g., reliability of a piece of software), simply measure the process used to develop that software using the *assumption* that better software processes produce better software. This is the concept used in the Software Engineering Institute's Capability Maturity Model (CMM) [8]. However, this assumption, although plausible, has never been shown to be true in any valid scientific experiment.

A second aspect of the measurement problem is that despite known methods for discovering errors [9] [13] and some studies analyzing the causes of failures [4], there is for the most part, no known correlation between process and product quality. As a result, it is imperative that CHISSA investigate and promote the experimentation, data collection, and measurement aspects of software development and assurance.

Because NIST is well-known for its ability to measure and conduct unbiased experiments on technology, CHISSA will adopt NIST practices as appropriate and will promote collaborative large-scale projects that will give industry the knowledge necessary to understand a specific technical approach's impact on their projects. CHISSA will provide guidance on how to convert research results into technology usable by industry.

2.2.2 Demonstration Facility

CHISSA will provide a mechanism for disseminating results by creatiing a Demonstration Facility, which will provide a resource at NIST with links to other relevant technology. NIST is recognized as a source of standard reference materials in other fields and can become the same type of source in software engineering. Software engineering has produced the equivalent of standard reference materials but they have not been widely presented and made available. The Demonstration Facility is described further in Section 3.1.

2.3 Long Term Goals

Measurement and technology dissemination are CHISSA infrastructure components. CHISSA's long term goal is to understand effective technologies for producing high integrity system software. While the white papers represented a cross section of different communities and views, some commonality was discovered among the problems faced by each. But there were also differences. This finding is supported by a recent Workshop on High Assurance Computing, sponsored by the Naval Research Laboratory (NRL), the Office of Naval Research, and the Advanced Research Projects Agency (ARPA) in February 1995. Experts from the fields of safety, security, real-time, and dependability (fault tolerance) attended.[1] These experts agreed that there are intersections where the same technology cuts across each interest area and there are conflicts too. They agreed that no single community (e.g., security for safety, fault tolerance, safety for security, fault tolerance for real time) can solve all the problems. The concept of high integrity software system assurance encompasses all the communities and associated problem areas.

Another aspect of understanding effective technologies is to identify the specific benefits of each method for each attribute, lifecycle process, and defect class relative to process and software / system product. It is a long term objective of CHISSA to identify the costs versus the benefits of selecting software methods for specific projects. NIST staff are currently exploring a rationale for defining and presenting this type of information to enable program managers and customers to make the decisions necessary for assuring software systems.

For each of these technical topics, CHISSA will assess the state of practice relative to current research, identify techniques proven to be useful, identify where research is needed to understand

[1]Proceedings from this Workshop are being prepared by NRL.

new technologies, and plan how to get the technology into widespread use. Guidelines for education, both in university currucula and industrial training, will be developed for transitioning such technologies into practice. The workshops described in Section 3.3 describe the mechanism CHISSA will use to understand industry needs.

3 High-Integrity Measurement and Evaluation

Software engineering lacks a strong experimental flavor that results in measurements of technology benefits. As such, new technology is generally evaluated on an ad hoc case-by-case basis. It becomes extremely difficult using this model to objectively demonstrate that a given tool, process, or mechanism really has an impact on the software product being developed. Before new technology can effectively be diffused throughout the industry, objective procedures must be developed for evaluating new technology. All too often "silver bullets" are proposed as magic solutions to software engineering problems, only to be discarded a few years later by new, more exotic silver bullets [1].

Technology transfer takes time. In an early study of software technology, Redwine and Riddle determined that new software technology often took from 15 to 20 years to become the state-of-the-practice [10]. No one technology, by itself, solves the problem. It is the collection of numerous small changes that evolve into new, useful technology.

In a related study within NASA, Zelkowitz studied the adoption of new software technology within a single government agency [15]. In this case, several technologies (e.g., Cleanroom, inspections, Ada) were tracked, and in each case, the adoption of that technology within the agency took several years with numerous instances of training, pilot studies, and evaluation activities. The process of change is labor and time intensive and is not the result of a single course, project, or lecture.

A theme occurring in all these technology transfer activities is the need to understand, quantify, and evaluate the effects of new technologies on the development process and products under construction. A significant force within the NASA work in understanding the technology transfer issues has been the NASA Software Engineering Laboratory (SEL), which was created at Goddard Space Flight Center (GSFC) in 1976 [7]. The SEL has been collecting data, running experiments, and evaluating software engineering technologies, and in the past 19 years has amassed a database of over 150 projects, which can be used to establish trends and to demonstrate the impact of new technologies on the software development process. The SEL approach has evolved to a three-level process in technology maturation:

- *Understand.* It is first necessary to understand the existing technology. Before it is possible to improve a process, one must be able to understand (i.e., measure) what one already has. Providing an initial baseline evaluation of existing technology is crucial for all future activities.
- *Assess.* Once a baseline is established, new technology can be evaluated. Given a database of baseline data, the impact of new technology can be appropriately understood. It is also a fact derived from 19 years of SEL research, that this task is extremely difficult. With software

projects often costing in the millions of dollars, it is simply not feasible to run multiple controlled experiments to determine the effects of a new technology. Also, due to the varying ability of project personnel, ability of the development staff also perturbs results.

- *Package.* Once a new technology has been evaluated, it must be tailored to the new organization and packaged in a manner usable by that organization. That includes training materials, guidebooks, standards, tools, etc. in the new technology. It is the packaging aspect that provides the transition of the technology to industry.

CHISSA must have components similar to the SEL, while taking advantage of the NIST history in statistical experimentation. Data must be collected across a broad segment of the industry using various methods and tools. A method for providing commonality in measurement must be developed; this method could simply be explanations relating each project's characteristics to measurements. The results must be such that they enhance understanding across different types of projects. Facilities for disseminating this information will provide a valuable resource that will aid future research. The major difference between the SEL and CHISSA is that the SEL is an internal organization of the Flight Dynamics Division of NASA/GSFC, while CHISSA will coordinate activities across various development groups in different organizations and researchers in still other organizations. It is CHISSA's role to play "matchmaker" between industry and researcher and to provide the repository where such research data and development tools can be stored, accessed, and disseminated.

This provides a direction for at least one of CHISSA's early workshops. The role of experimentation and data collection and measurement will be the focus of a workshop to be held in November 1995, as described in Section 3.3. Processes for collecting such data and providing access to it on CHISSA's demonstration facility are early work items for CHISSA.

3.1 Demonstration Facility

A CHISSA goal is to accelerate the acceptance and use of high integrity software system assurance technology by industry. One of the main themes from the white papers is that often industry is unaware of existing technology and the total base of knowledge surrounding that technology. A concrete example of this occurred at a recent conference,[2] where an expert in software verification and validation gave a presentation to a group of people in a specific aspect of the health care industry. The presentation included discussion of standards to help people develop and assure their software. When the audience appeared somewhat blank-faced, the speaker asked if they were familiar with software engineering standards. Only a few raised hands, and of those, as it came out in discussion, most knew only of the IEEE standard on software verification and validation through FIPS PUB 132 [3] on software verification and validation.

CHISSA will build a demonstration facility on the internet to make the results of CHISSA activities available to a large audience. Initial plans are to create a WWW site for browsing among

[2] Private conversation with Dolores Wallace and Roger Fujii, Logicon

available data. Creation of this demonstration facility requires addressing the following issues discussed below.

3.1.1 Taxonomy of high integrity issues

A classification model will need to be developed for navigating through the WWW site. For example, the following could represent a preliminary classification. A user would choose one or more from each category:

Attribute. These are the high-integrity attributes of interest. Example attributes could be safety, security, reliability, fault tolerance, or correctness.

Life cycle phase. The user would indicate the phase or process of the life cycle of concern. Examples could be requirements analysis, design, coding, or testing.

Defect classes. These define the particular issue to be addressed. Examples of defect classes could be items such as logic errors, performance problems, or schedule slippage.

The results of this taxonomy are *techniques and metrics* applicable to the chosen categories. The user would query the WWW site (e.g., "I have a *schedule problem* in the *design* phase of a *security* system.") The response would be a link to a series of papers, tools, and other references dealing with [security, design, schedule] concerns (Figure 2).

3.1.2 Interactive tool demonstration

The result of the query process on the CHISSA WWW site is a pointer to an appropriate set of techniques and metrics that address the concerns of the user with pointers to the elements shown in Figure 2. Tools supporting these techniques and metrics would be available for access via the WWW. Although it would be possible for this to be a physical entity at a unique location, CHISSA will distribute this information across the internet to:

- eliminate the need for NIST personnel to be able to demonstrate any tool, any time, on demand;
- distribute the required staffing across all suppliers of demonstrated tools; and
- provide access to the CHISSA WWW services by using the internet without the need to come to the facility.

The demonstration facility will be constructed on top of the WWW, which is widely available, becoming a standard, capable of dealing with demonstrations in a wide variety of forms, and has good search and exploration capabilities. The facility will be "hosted" at NIST, though due to

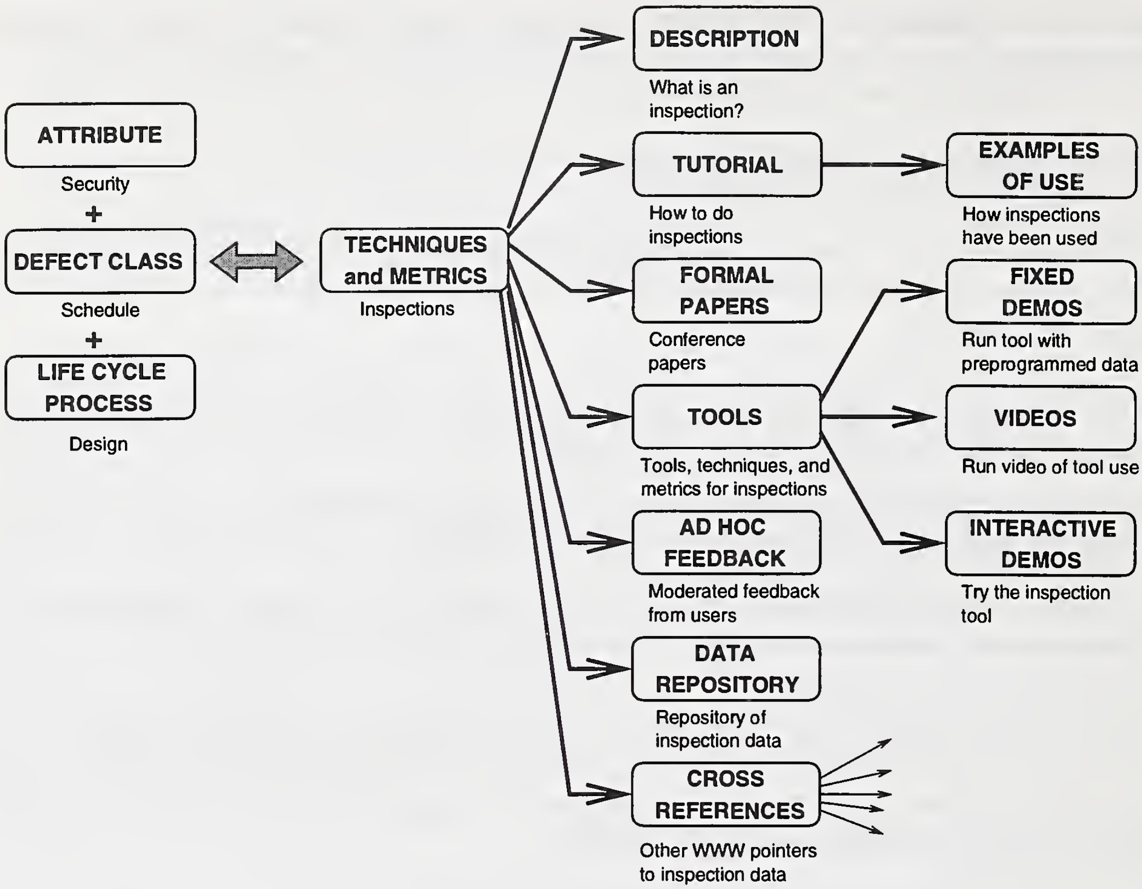

Figure 2: Techniques and Metrics for Inspections.

the hyperlink nature of the WWW, the contents will be distributed. Papers, reports, product demonstrations, and courseware will all be available.

Using the hyperlinks of the WWW, the user will:

- Find a process description of current "best practices" for this topic. This would provide tutorial information about how high integrity has been achieved by others with similar problems.
- Find papers, research reports, and observations about the current topic of interest.
- Access a tool demonstration that addresses automation of the process.
- Provide access to the measurement database that will allow others to compare their own measurement data with the baseline data that CHISSA has collected on the topic.

Populating this taxonomy with appropriate reports, metrics, tools, and data will be a major output for CHISSA for years to come. While some of these items will be developed at NIST, much will be produced by the organizations with which CHISSA will work. Many items already exist and will need only to have reference links.

On-line tutorials and three forms of tool demonstration are initially being considered for this facility:

1. A video is run showing use of the tool and its effects upon the topic of interest.
2. A preplanned demonstration is executed using the tool with preprogrammed data to allow the user to manipulate the tool with the given data. This provides more of a "look and feel" for using the tool.
3. The user uses the tool with the user's own data. This allows the user to try the tool in a more realistic setting.

The live demonstration with user data is a long term goal of the demonstration facility. However, CHISSA must determine the feasibility of developing such a demonstration ability that will execute a large assortment of contributed tools using existing WWW servers and browsers such as Mosaic and Netscape.

Prototype Demonstration Facility. The software inspection process is the technology to be studied first, as a demonstration of concept. NIST has published a document containing checklists for a specific application domain. NIST already has a Memorandum of Understanding (MOU) with NASA's IV&V Facility, who can help link up to NASA's wealth of guidance and experience with software inspections. The wealth of information, including measurement, on software inspections, makes it an easy candidate for building a prototype of how the demonstration facility will function. NIST is providing the code analysis tool, **unravel** [6] that performs slicing[14] over C-language programs. This provides a way to audit code as part of the inspection process.

It is proposed that CHISSA will work with various NASA sites (e.g., the Jet Propulsion Laboratory (JPL), the Langley Research Center (LaRC), and the SEL at Goddard Space Flight Center (GSFC)) to study inspections. A repository will be developed on the WWW with the help of the Software Engineering Institute (SEI) in Pittsburgh, PA, and the MITRE Corporation. Additional work by Philip Johnson at the University of Hawaii will be incorporated into the demonstration facility.

CHISSA participants are currently working to:

- Develop an example taxonomy of the inspection process to provide an agent the ability to browse.
- Customize a WWW browser to permit the interaction with tools such as **unravel**.
- Develop an experiment that uses **unravel** in an inspection environment and collect data on the effectiveness of using such a tool.
- Build a repository of collected papers on the inspection process that is to be available on the WWW.

This testbed will examine what can be accomplished to make this long-distance demonstration possible.

3.1.3 Tool Repository

A longer-range goal is to populate the demonstration facility with other tools that support the production of high integrity software. Of particular concern is the requirement to make good research and prototype tools available for study and evaluation without implying NIST endorsement of a particular product. Still unclear is whether CHISSA should develop criteria describing which tools are to be allowed within the WWW site or "caveat emptor" with CHISSA making any tool available as long as certain demonstration criteria are met.

Since use of the facility is a human computer interface problem, it may be useful to conduct local experiments to see how well people navigate through the facility. A well-designed human computer interface will be invaluable for the information transfer envisioned.

3.1.4 Measurement

CHISSA will provide information on usage of the tools: either case studies from other sources or as results of laboratory study. In addition, as CHISSA evolves as the coordinator of experimental research with various industrial organizations, it is important that the lessons learned from such experiments not be lost. Project reports, data, and evaluations from the various studies conducted will be placed in the repository and made available on the WWW.

3.1.5 Fostering Research

The concept of a repository of industrial challenges comes from the observation that, at some point, understanding technology requires work on large systems like Air Traffic Control instead of applying concepts to "toy problems." The repository will facilitate this by providing a repository of perhaps "sanitized" real world examples of high assurance challenges. This would enable researchers to develop tools and techniques and apply the tools and techniques to real data.

Another use for the repository will be as a source of case studies. Much like Peter Neumann's "Risks of Computing," on the internet, a source of real-world dependability related problems can serve as both an inspiration to researchers and as a sales tool to convince upper-level management of the need to use methods for dependability.

Finally, we may populate the repository with "grand challenges" and try to coordinate industries who wish to work on them. For formal methods, examples of grand challenges might include a formally verified Ada compiler or a complete formal proof of any real system.

3.2 CHISSA As Facilitator

Under today's economic climate, it is doubtful whether CHISSA will be able to sponsor many of its own research activities. Therefore, an important component of CHISSA activities will be to facilitate such research being sponsored by other agencies. CHISSA will make its views known to these agencies.

CHISSA will provide the clearinghouse, through workshops, conferences, and publications, to facilitate industry and university meeting to develop projects of mutual benefit. Industry must understand that its problems are amenable to academic study, and the academic world needs to know what the industrial problems are as a source of interesting research issues. CHISSA will provide the forum for both groups to meet.

Working in concert with these groups will allow CHISSA to leverage its knowledge and resources to a wide audience. A long term goal of CHISSA is to become the national resource in the experimentation, collection, and evaluation of software engineering research toward creation of high integrity software systems.

3.3 Workshops

Three types of workshops will serve in the short term for the purpose of technology transfer. Each category has a different purpose and is intended to serve a different audience. The types are Industry Focus Area Workshops, Technology Diffusion Workshops, and Topical Workshops.

3.3.1 Industry Focus Area Workshops

Industry Focus Area Workshops are one-day workshops to expose managers (e.g., executive level, high-level system designers, regulators, high-level acquisition officers) to the problems and technologies available for the development of high integrity software systems. The purpose is to help participants understand these technical challenges. The workshops will encourage speakers with horror stories and speakers describing solution technologies, in a non-technical, understandable, manner. The attendees will better understand why there is a need to develop high integrity software systems, why it is important to do so, and with a set of reasonable expectations as to what the technology can accomplish. It is not the purpose of these workshops to provide the technical details of solutions to these problems, but instead, to provide industrial leaders information on where to look for possible solutions to their problems.

Feedback from attendees will be used to help guide CHISSA. It will provide information useful for developing the other two classes of workshops and for developing a CHISSA research and development program.

These workshops will provide attendees with contacts for possible followup of either available technology or individuals or institutions available for research and development on these ideas.

Finally, the attendees will perceive that CHISSA has provided a valuable service to the community. CHISSA should come away with a better understanding of the technical problems that industry must resolve. These industry focus area workshops will be heavily publicized and may be repeated in different cities. Expected audience size is 100. Likely locations could be Washington, D.C., Boston, Silicon Valley, Los Angeles, Austin or other cities with many organizations producing high integrity software systems. It is possible that the workshop could be videotaped for shipment to other organizations or for use on the WWW. This workshop could be planned for a two-year cycle. There would need to be a mechanism to ensure feedback on the value of the workshop. The Steering Committee's planned attendance at the first workshop will lend credibility to the event and offer the Steering Committee an opportunity for direct assessment of its value. Individual Steering Committee members may attend subsequent workshops for continued visibility and evaluation.

The first workshop is planned for September 21, 1995. Initial plans are now being made for this meeting, which will be held at Loral Federal Systems in Rockville, MD.

3.3.2 Technology Diffusion Workshops

This paper presents some initial ideas of how CHISSA will operate and provide the technology transfer mechanisms required by the software industry for high integrity software. Technology Diffusion Workshops will enable CHISSA to evolve these mechanisms to best help industry use the results of research with a minimum of delay. Unlike Focus Area workshops, these will be invitational, with a goal of no more than 50 participants. This is a flexible goal, because the topic areas are broad enough that a larger group could be split into subgroups each addressing a component of the topic. These workshops may be held 2 to 4 times a year, each addressing a single topic. Both practitioners and researchers will attend, with each community airing its problems and both striving toward solutions. These workshops are intended to impact the manner in which the research community selects research topics, develops approaches to solutions, experiments with and evaluates the results of that research, and packages the results. These may also lead to some partnerships. Suggested topics, by no means inclusive, include:

1. Providing for better experimentation, data collection, and analysis in the software development process in order to improve the development process.

2. Building data repositories and development mechanisms for the collection, evaluation, and use of development data.

3. Managing and fostering technology transfer to provide researchers with a supply of relevant problems to discuss, and to provide industry with mechanisms for learning about the effectiveness of new technology.

4. Developing university and continuing education processes that provide for the continual improvement of the level of knowledge of the technical work force.

5. Developing industrial strength problems or "Grand Challenges" needing solutions is CHISSA's goal for high integrity systems.

6. Developing methods for technology standardization as a means to disseminate good practices without stifling a fast moving industry. With product lifecycles on the order of two to three years, and ANSI / ISO standardization taking 4 to 6 years in many cases, the classical voluntary consensus standardization process is becoming increasingly less relevant. Consortia (e.g., OSF, OMG) and proprietary (e.g., Microsoft's OLE) standards, as well as ANSI, IEEE and ISO standardization mechanisms must address the needs for high integrity software.

These workshops will not address specific technologies (e.g., reuse of code, formal methods, verification), but instead address broader procedural issues in the management of CHISSA goals. One problem will be whom to invite. While the academic community is fairly well connected, industry is more diverse. Who are the most appropriate persons to invite from the industrial world.

Because of the importance of experimentation, data collection, and measurement, the first of these technology diffusion workshops will have these as a theme. Bringing together the research measurement community, companies currently heavily involved with data collection and evaluation, and companies wishing to be so involved, should provide an initial focus on data CHISSA needs to collect.

The first of these workshops is currently planned for November, 1995.

3.3.3 Topical Workshops

These workshops will provide the detailed technical knowledge required for solving real industrial problems. Researchers and industry users will provide the " state of the practice" on specific technologies (e.g., reuse, formal methods, process modeling), with subsequent discussion relating to the impact on the high integrity attributes, what's missing from current technology, and where industry can go to continue improvement. This will be an important leadership role for CHISSA. CHISSA could play the role of "marriage broker" in bringing together researcher and industry in order to create partnerships for experimentation on development activities. Industry can provide the real-world expertise to keep the academic research "honest" and relevant.

Ideas for creating such linkages could include:

- Short proposals from industry on what it needs
- Short proposals from the university on what it would like to do
- Concepts from industry still needing answers, which could lead to new Ph.D. dissertation topics
- Submission of artifacts (e.g., testing tools) from developers. CHISSA could help the technology transfer activity by adding such tools to its WWW repository, as long as "NIST endorsement" issues are addressed.

It is important that industry provide industrial strength problems needing solutions at each workshop. The format could be perhaps 6-8 industrial presenters and 6-8 academic presenters. Government, regulators and acquisition issues must be addressed as well.

4 Summary

CHISSA is developing plans for a group of activities intended to address the major issues identified in an initial submission of 94 white papers. The principal task is disseminating information to industry, in a form that is usable by industry, on problems that will help industry to produce high integrity software systems in a cost-effective manner.

Among the mechanisms CHISSA will use to accomplish this task are:

- An experimental laboratory to facilitate academic research and industrial organization co-operation and to provide a repository for the collection and dissemination of experimental data.
- An interactive demonstration facility available on the World Wide WWW for exhibiting tools, and other published documentation, in an easily accessible manner.
- One-day workshops directed toward providing industry with solutions and receiving feedback from industry on problems needing solutions.
- Two-days workshops to aid in developing mechanisms for the diffusion of new technology usable by industry and government.
- Other workshops and conferences that address technical topics; these may be proposed or promoted by CHISSA but conducted by other organizations.
- Collaboration with funding agencies.

Once several of these mechanisms are in place, CHISSA will focus on long term Grand Challenges leading toward solutions for high integrity software system assurance.

References

[1] Brooks, F., No Silver Bullet: Essence and Accidents of Software Engineering, *IEEE Computer* (20)4, (1987), 10-19.

[2] Fenton N., S. Pfleeger, and R. Glass, Science and Substance: A Challenge to Software Engineers, *IEEE Software*, (11)4, (1994), 86-95.

[3] FIPS PUB 132, *Guideline for Software Verification and Validation Plans,* U.S. Department of Commerce/National Bureau of Standards (U.S.), (November 19, 1987).

[4] Hecht, H., Rare Conditions — An Important Cause of Failures, 8^{th}IEEE Annual Conference on Computer Assurance, (June 1993).

[5] Knight J. and D. Kienzle, Preliminary Experiences Using Z to Specify a Safety-Critical System, *Proc. 1992 Z Users Workshop*, (1992).

[6] Lyle J., et al, Unravel: A CASE Tool to Assist Evaluation of High Integrity Software, NIST, (*To Be Published as a NIST IR*).

[7] McGarry F., R. Pajerski, G. Page, S. Waligora, V. Basili and M. Zelkowitz, Software process improvement in the NASA Software Engineering Laboratory, Software Engineering Institute TR CMU/SEI-94-TR-22, (December 1994).

[8] Paulk M. C., B. Curtis, M. B. Chrissis and C. V. Weber, Capability Maturity Model for Software, Version 1.1, *IEEE Software*, (10)4, (July 1993), 18-27.

[9] Peng, Wendy W., D. R. Wallace, *Software Error Analysis*, NIST SP 500-209, U.S.Department of Commerce/National Institute of Standards and Technology, (April 1993).

[10] Redwine S. and W. Riddle, Software technology maturation, 8^{th} IEEE/ACM International Conference on Software Engineering, London, UK, (August 1985), 189-200.

[11] Wallace D., L.M. Ippolito, D.R. Kuhn, *High Integrity Software Standards and Guidelines*, NIST SP 500-204, U.S. Department of Commerce/ National Institute of Standards and Technology, (September, 1992).

[12] Wallace D., Peng W., Ippolito L., Software Quality Assurance: Documentation and Reviews, NIST, NISTIR 4909, U.S. Department of Commerce/National Institute of Standards and Technology, (September 1992).

[13] Wallace, Dolores R., *Verification and Validation*, *Encyclopedia of Software Engineering*, John Wiley & Sons, Inc., New York, (1994).

[14] Weiser, M. Program slicing, *IEEE Transactions on Software Engineering*, (10)7, (1984), 352–357.

[15] Zelkowitz M. V., Assessing Software Engineering Technology Transfer Within NASA, Technical Report NASA-RPT-003-95, NASA/GSFC, (January 1995).

Appendix A. CHISSA Information

- CHISSA Program Manager:
  Mrs. Dolores Wallace
  National Institute of Standards and Technology
  Room B266, Technology Building
  Gaithersburg, MD 20899
  Internet: dwallace@nist.gov
  Fax: (301) 926-3696
  Telephone: (301) 975-3340

- CHISSA Steering Committee:

Ms. Dolores Wallace	NIST
Mr. Jon Dehn	Loral Corporation
Ms. Helen Gill	National Science Foundation
Dr. George Gilley	Aerospace Corporation
Mr. Charles Howell	Mitre Corporation
Dr. John Knight	University of Virginia
Dr. Gary Koob	Office of Naval Research
Dr. Joseph Profeta	Union Switch and Signal
Dr. John Salasin	Advanced Research Projects Agency
Dr. Fred Schneider	Cornell University
Dr. Dan Siewiorek	Carnegie Mellon University
Dr. Charles Weinstock	Software Engineering Institute

- Dr. Marvin V. Zelkowitz, NIST and University of Maryland

Appendix B. CHISSA Focus Areas

A. INFRASTRUCTURE ISSUES:

1. Standards
   Applicable standards for high-integrity systems
   Role of standards in high integrity system design

2. Experimental methodologies
   How to do experimentation
   How to represent experimental data

3. Education
   University curriculum
   Methods for continuing education

4. Technology Transition
   CHISSA laboratory facility to demonstrate tools
   How CHISSA transfers technology to industry
   Processes involved in technology transfer
   Meetings and workshops for purpose of technology transfer

B. FUNDAMENTAL TECHNOLOGIES:

1. Formal methods
   Using formal methods
   Formal requirements analysis
   Computational requirements

2. Languages
   Syntax and semantics for languages
   Specification and requirements languages

3. Measurement technology
   Data collection guidebook
   Repository of collected valid data
   Models of software complexity, reliability, etc.

4. Theory
   Development of models and metrics of high-integrity systems

5. Process
   Report on relationship between process and product
   Methodology for high integrity system design
   Process evolution

C. ENGINEERING TECHNOLOGIES:

1. Requirements analysis tools
   - Tools for requirements and specifications
   - Traceability of requirements

2. System design
   - Criteria for high integrity systems
   - Frameworks for high integrity systems
   - Architectures for large and evolving systems
   - Distributed systems & communication protocols

3. Assurance
   - Security
   - Safety analysis
   - Fault analysis
   - Fault tolerance
   - Risk analysis
   - Human Computer interfaces

4. Validation and Evaluation
   - Guidebook on testing
   - Third-party certification
   - Intelligent systems
   - Field analysis of tools
   - High integrity documentation
   - Use of formal standards specifications for conformance tests

5. Engineering management
   - How to do reverse engineering
   - Reusing modules
   - Formal methods on legacy code
   - Effective use of COTS products
   - Semantic modeling of components

Appendix C. White Paper Sources

Of the 94 white papers were submitted to CHISSA in late 1994-early 1995, many represented collaborative efforts among several organizations. In some cases, different individuals within the same organization submitted separate papers. The following list identifies the organizations who submitted white papers:

AT&T Bell Labs
Aerospace Corp.
ANALYSIS
Azor, Inc.
Brookhaven Technology Group
CPI
Carnegie Mellon University
Colorado State University
DePaul University
Eastern Nazarene College
George Mason University
Georgia State University
Hanscom Air Force Base
IBM
J. F. Taylor, Inc.
Logicon
Michigan State University
NASA Jet Propulsion Laboratory
NASA Langley Research Center
National Security Agency
New York University
North Carolina State University
Opsimath Research
Portland State University
Prism Program, Hanscom AFB
Reliable Software Technology
Rockwell, Intl.
Siemens
SoHaR Inc.
Software Quality Engineering
Storage Technology Corp.
Tandem Computer
The Boeing Company
Trusted Information Systems
University of Alabama at Huntsville
University of California - San Diego
University of Hawaii
Advanced Information Microstructures
Alliedsignal Aerospace
Averill and Associates
BNR
CACI, Inc
CTA, Inc.
City University, London
Computational Logic Inc.
Decitek, Inc.
Food and Drug Administration
Georgia Institute of Technology
Grumman
Hughes Aerospace & Electrical Corp.
Institute for Defense Analyses
Lockheed Martin Mgmt & Data Systems
Loral Air Traffic Control
NASA Ames Research Center
NASA Johnson Space Center
NIST
Naval Postgraduate School
North Carolina A&T State University
Ohio State University
Polytechnic University of NY
Praxis Systems
Redstone Arsenal (U.S. Army)
Rocksoft LTD
Sandia National Laboratories
Skidmore College
Software Engineering Institute
Southwest Research Institute
SUNY at Stony Brook
Texas A & M University
The Mitre Corp.
United Defense
University of California - Los Angeles
University of California - Santa Barbara
University of Houston - Clear Lake

University of Iowa
University of Ottawa
University of York
WW Technology Group
Westinghouse Electric Corp.
University of Maryland - College Park
University of Pennsylvania
University of Texas at Austin
West Virginia University

CHISSA values these contributions and welcomes continued input from the community at large. Comments about CHISSA's program should be submitted to Mrs. Dolores Wallace, CHISSA Program Manager, at the address given in Appendix A.

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899-0001