

FY 2001 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in previous ITL Technical Accomplishment reports are not repeated.

Author	Title	Place of Publication	Date
Alpert, B., Greengard, L., Hagstron,	Nonreflecting Boundary Conditions for the Time-Dependent Wave Equation	Journal of Computational Physics	
<p>We describe a new, efficient approach to the imposition of exact nonreflecting boundary conditions for the scalar wave equation. We compare the performance of our approach with more standard boundary conditions by coupling them to finite difference schemes. Numerical experiments demonstrate a significant gain in accuracy at no additional cost.</p>			
Anderson, D. M., McFadden, G. B., Wheeler, A. A.	A Phase-Field Model with Convection: Sharp-Interface Asymptotics	NISTIR 6568 and Physica D	10/25/2000
<p>We have previously developed a phase-field model of solidification that includes convection in the melt. This model represents the two phases as viscous liquids, where the putative solid phase has a viscosity much larger than the liquid phase. The object of this paper is to examine in detail a simplified version of the governing equations for this phase-field model in the sharp-interface limit to derive the interfacial conditions of the associated free-boundary problem. The importance of this analysis is that it reveals the underlying physical mechanisms built into the phase-field model in the context of a free-boundary problem and, in turn, provides a further validation of the model. In equilibrium we recover the standard interfacial conditions including the Young-Laplace and Clausius--Clapeyron equations that relate the temperature to the pressures in the two bulk phases, the interface curvature and material parameters. In nonequilibrium we identify boundary conditions associated with classical hydrodynamics, such as the normal mass flux condition, the no-slip condition and stress balances. We also identify the heat flux balance condition which is modified to account for the flow, interface curvature and density difference between the bulk phases. The interface temperature satisfies a nonequilibrium version of the Clausius--Clapeyron relation which includes the effects of curvature, attachment kinetics and viscous dissipation.</p>			
Bace, R., Mell, P.	Intrusion Detection Systems	NIST SP 800-31(http://csrc.nist.gov/publicati)	8/1/2001
<p>Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. As network attacks have increased in number and severity over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. This guidance document is intended as a primer in intrusion detection, developed for those who need to understand what security goals intrusion detection mechanisms serve, how to select and configure intrusion detection systems for their specific system and network environments, how to manage the output of intrusion detection systems, and how integrate intrusion detection functions with the rest of the organizational security infrastructure.</p>			
Badre, A., Laskowski, S.J.	The Cultural Context of Web Genres: Content vs. Style	Human Factors and the Web 2001 Conference	6/6/2001

The question we raise here is whether what is culturally established for a given genre in the brick and mortar world applies equally on the World Wide Web. Can we effectively use the styles of one genre to design the site of another genre? Are we wedded to the culturally established attributes of the real world when designing for the Web? We compared users' performance and preference for shopping- vs. news-styled sites. We found that on the whole users liked the "shopping" layout better than the news layout, even when viewing news content. This was especially surprising in light of the fact that our users had so much more experience with news sites over shopping sites. This perhaps shows how popular the shopping style is in our culture. People chose News as Shopping as their favorite site, even though it was difficult to use. People who preferred News as Shopping did better on both News as Shopping and News as News, than those who preferred News as News. This suggests a potential relationship between performance on the World Wide Web and preference for the shopping style.

Author	Title	Place of Publication	Date
Barker, E.B.	Cryptographic Protection for the Twenty-First Century	Internet Security Conference Newsletter (TISC Insight), Volume 3, Issue 5, March 9, 2001	3/9/2001
<p>In 2000, the National Institute of Standards and Technology (NIST) announced the selection of a new encryption algorithm that will be used to protect sensitive (unclassified) government information. This algorithm, to be proposed as the Advanced Encryption Standard (AES), is the result of work conducted by NIST and the international cryptographic community since 1997. The AES is intended to replace the Data Encryption Standard (DES) that was adopted in 1977 and is now considered to be inadequate to protect today's information. However, the AES will not be used alone, but as part of a cryptographic standards toolkit of algorithms and protocols to provide security for various applications and environments.</p>			
Barker, E.B.	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	ITL Bulletin, December 2000	12/15/2000

Random and pseudorandom numbers are needed for many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures or for generating challenges in authentication protocols. NIST Special Publication (SP) 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, discusses the randomness testing of random number and pseudorandom number generators (RNGs and PRNGs) that may be used for many purposes including cryptographic, modeling and simulation applications. The focus is on those applications where randomness is required for cryptographic purposes such as the generation of keying material. A set of statistical tests for randomness is described in this publication.

Computational Science
(Springer-Verlag Lecture Notes in
Computer Science 2073), San
Francisco, California, May 28-30,
2001, pp. 629-632

REGTET, a Fortran 77 program for computing a regular tetrahedralization for a finite set of weighted points in 3-dimensional space, is discussed. REGTET is based on an algorithm by Edelsbrunner and Shah for constructing regular tetrahedralizations with incremental topological flipping. At the start of the execution of REGTET a regular tetrahedralization for the vertices of an artificial cube that contains the weighted points is constructed. Throughout the execution the vertices of this cube are treated in the proper lexicographical manner so that the final tetrahedralization is correct.

Bird, S., Day, D., Garofolo, J.,
Henderson, J., Laprun, C.,
Lieberman, M.

ATLAS: A Flexible and Extensible
Architecture for Linguistic Annotation

Second International Conference on
Language Resources and
Evaluation (LREC), Athens,
Greece, May 31-June 2, 2000

We describe a formal model for annotating linguistic artifacts, from which we derive an application programming interface (API) to a suite of tools for manipulating these annotations. The abstract logical model provides for a range of storage formats and promotes the reuse of tools that interact through this API. We focus first on "Annotation Graphs", a graph model for annotations on linear signals (such as text and speech) indexed by intervals, for which efficient database storage and querying techniques are applicable. We note how a wide range of existing annotated corpora can be mapped to this annotation graph model. This model is then generalized to encompass a wider variety of linguistic "signals" including both naturally occurring phenomena (as recorded images, video, multi-modal interactions, etc.) as well as the derived resources that are increasingly important to the engineering of natural language processing systems (such as word lists, dictionaries, aligned bilingual corpora, etc.). We conclude with a review of the current efforts towards implementing key pieces of this architecture.

Blackburn, M., Busser, R.,
Nauman, A., Chandramouli, R.

Model-Based Approach to Security Test
Automation

2001 Quality Week Conference,
San Francisco, California

Security functional testing is a costly activity typically performed by security evaluation laboratories. These laboratories have struggled to keep pace with increasing demand to test numerous product variations. This paper summarizes the results of applying a model-based approach to automate security functional testing. The approach involves developing models of security function specifications (SFS) as the basis for automatic test vector and test driver generation. In the application, security properties were modeled and the resulting tests were executed against Oracle and Interbase database engines through a fully automated process. The findings indicate the approach, proven successful in a variety of other application domains, provides a

Blue, J. L.

Fair Selection of Jury Panels from Jury
Pools

NISTIR 6569

10/25/2000

A standard problem of courts at all levels is the selection of a panel of potential jurors from a jury pool, which is a list of people who are eligible to serve as jurors. The problem is to select N people out of the M possible people in a fair way. One definition

of “fair” is that each of the M people has an equal chance to be selected for any jury pool. A much more rigorous definition is that each of the possible combinations of N people has an equal chance to be selected as the entire jury pool. A working computer program incorporating a fair algorithm for the problem stated above has been produced, together with a brief testing program. The properties of this algorithm are discussed, and an improved version of a program developed previously is

Author	Title	Place of Publication	Date
Boisvert, R. F., Donahue, M. J., Lozier, D. W., McMichael, R., Rust, B. W.	Mathematics and Measurement	NIST Journal of Research, Vol. 106, No. 1, January-February 2001	2/28/2001
<p>In this paper we describe the role that mathematics plays in measurement science at NIST. We first survey the history behind NIST's current work in this area, starting with the NBS Math Tables project of the 1930s. We then provide examples of more recent efforts in the application of mathematics to measurement science, including the solution of ill-posed inverse problems, characterization of the accuracy of software for micromagnetic modeling, and in the development and dissemination of mathematical reference data. Finally, we comment on emerging issues in measurement science to which mathematicians will</p>			
Boisvert, R. F., Moreira, J., Philippsen, M., Pozo, R.	Numerical Computing in Java™	Accepted by Computing in Science and Engineering	
<p>We discuss the advantages and disadvantages of using Java(TM) for numerical computing. We provide examples of current performance levels and propose several additional language features that would make Java more easily applied in scientific</p>			
Boisvert, R., Lozier, D.	Handbook of Mathematical Functions	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 135-139.	1/31/2001
Burr, W.E.	Data Encryption Standard	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 250-253	1/31/2001
Burr, W.E.	Digital Rights Management: How Much	Included in NISTIR 6591, Digital	1/11/2001

Cryptography offers powerful techniques for data protection in "classical" communications applications. Claims are often made that some new "technology" will enable or make electronic publishing "safe." This talk sounds a cautionary note, at least for large scale, controlled distribution of digital content to millions of consumers or subscribers. The essential difference is that both the sender and the receiver are trusted parties in a communications protocol (an attacker is a third party), but in Digital Rights Management (DRM) applications the consumer who receives the data is the likely attacker. This is a much more difficult problem. Cryptography may also offer small comfort to traditional intellectual property rights holders in the face of changing ethics and notions of property rights, and evolving business models, all of which are driven by new digital technologies.

Author	Title	Place of Publication	Date
Carasso, A.S.	The Apex Method in Image Sharpening and the Use of Low Exponent Lévy Stable Laws	NISTIR 6749 and SIAM Journal on Applied Mathematics	5/30/2001

The APEX method is an FFT-based direct blind deconvolution technique that can process complex high-resolution imagery in a few minutes of cpu time on current desktop platforms. The method is predicated on a restricted class of shift-invariant blurs that can be expressed as finite convolution products of two-dimensional radially symmetric Lévy stable probability density functions. This class generalizes Gaussian and Lorentzian densities but excludes defocus and motion blurs. Not all images can be enhanced with the APEX method. However, it is shown that the method can be usefully applied to a wide variety of real blurred images, including astronomical, Landsat and aerial images, MRI and PET brain scans, and scanning electron microscope images. APEX processing of these images enhances contrast and sharpens structural detail, leading to very noticeable improvements in visual quality. The discussion includes a documented example of non-uniqueness where distinct point spread functions produce high-quality restorations of the same blurred image. Significantly, low exponent Lévy point spread functions were detected and used in all the above examples. Such low exponents are exceptional in physical applications where symmetric stable laws appear. In the present case, the physical origin of these Lévy exponents remains uncertain.

Chandramouli, R.

A Framework for Multiple Authorization
Types in a Healthcare Application

17th Annual Computer Security
Applications Conference (ACSAC),
New Orleans, Louisiana, December
10-14, 2001

In most of the current authorization frameworks in application systems, the authorization for a user operation is determined using a static database like ACL entries or system tables. These frameworks provide cannot provide the foundation for supporting multiple types of authorizations like Emergency Authorizations, Context-based Authorizations etc, which are required in many vertical market systems like healthcare application systems. In this paper we describe a dynamic authorization framework which supports multiple authorization types. We use the acronym DAFMAT (Dynamic Authorization Framework for Multiple Authorization Types) to refer to this framework. The DAFMAT framework uses a combination of Role-based Access Control (RBAC) and Dynamic Type Enforcement (DTE) augmented with a logic-driven authorization engine. The application of DAFMAT for evaluating and determining various types of authorization requests for the Admissions, Discharge and Transfer System

Chandramouli, R., Marshall, G.

Admission, Discharge, and Transfer
System Protection Profile (ADT-PP) (An
ISO/IEC 15408 Security Protection
Profile for a Healthcare IT Application

NISTIR 6782

8/22/2001

The central piece of information in this document is a set of security functional and assurance requirements for an Admissions Discharge and Transfer System (ADT). The ADT is a key information technology (IT) application system used in all major healthcare settings and is the first point of electronic capture of all individually identifiable healthcare information. The set of security functional and assurance requirements is expressed in a format that conforms to the "Protection Profile" (PP) framework that is the part of the ISO/IEC 15408 security criteria. The underlying motivation in developing the Admissions, Discharge and Transfer System PP (referred to ADT-PP) is to demonstrate the use of a protection profile as a vehicle for capturing the dictates of public policy regulatory requirements in the form of IT application system security specifications (consisting of both security functional and assurance requirements) for healthcare IT application systems. Expressing the IT application system's security specifications in a common standardized framework would facilitate the process of interpreting the regulatory requirements among the stakeholders as well as provide a common vocabulary to support subsequent processes like design, development and evaluation of systems. The deployment of such systems in healthcare settings would then serve to meet the underlying goals of the security policy regulation – namely the integrity, availability, confidentiality and privacy of individually identifiable healthcare information."

Chang, W.L.

The Design and Implementation of
MPEG-7 Collaboration Annotation Tool

Seventh International Conference
on Distributed Multimedia System
DMS2001, Tamkang University,
Taipei, Taiwan, September 26-28,
2001

The XML metadata technology of describing Web objects has emerged as a dominant mode of making information available both for human and machine consumptions. To realize this promise, many online Web applications are pushing this concept to its full potential. However, a good metadata model does require a good standardization effort so that the metadata content and its structure can reach its maximum usage between various applications. An effective collaboration annotation tool should also use

standard metadata structures in order to impact the enterprise collaboration environment. A new metadata technology called MPEG-7 content description has taken off from the ISO MPEG standards body with the charter of defining standard metadata to describe audiovisual content. This paper presents the design and implementation of a prototype tool, MCAT, which is able to annotate audiovisual objects using standardized content description metadata so that annotations can be shared between other

Author	Title	Place of Publication	Date
Chang, W.L.	Standard Metadata for Multimedia	2001 Symposium on Document Image Understanding Technology	

The XML metadata technology of describing online documents has emerged as a dominant mode of making information available both for human and machine consumptions. To realize this promise, many online Web applications are pushing this concept to its full potential. However, a good metadata model does require a robust standardization effort so that the metadata content and its structure can reach its maximum usage between various applications. An effective document content understanding should also use standard metadata structures especially when dealing with multimedia contents. A new metadata technology called MPEG-7 content description has taken off from the ISO MPEG standards body with the charter of defining standard metadata to describe audiovisual content. This abstract session will give an overview of MPEG-7 technology and what impact it can bring forth to the next generation of multimedia indexing and retrieval applications.

Ciarletta, L.P., Dima, A.A., Iordanov, V.P.	Using Intelligent Agents to Assess Pervasive Computing Technologies	Proceedings of the International Conference on Intelligent Agents, Web Technology, and Internet Commerce (IAWTIC'2001)	
---	---	--	--

Pervasive Computing (a.k.a. Ubiquitous or Ambient Computing) is a new field of computer science generally considered to lie at the intersection of desktop computing, networking, and embedded systems. Related to pervasive computing are Intelligent Environments and Smart Spaces. Intelligence is associated with the responsiveness, the ability to adapt and the ability to learn of the networked, computerized devices, and appliances that populate the user's environment. Unfortunately, the ongoing efforts in the industry are mainly focused on applications and devices that explore short-term technical issues, and there is no standard definitions or even agreements on the common vocabulary associated with these technologies. Pervasive computing is mainly about creating computerized and networked environment that will help the user to perform technical tasks and to help with daily "chores". Human Computer Interaction is therefore another important research area of the Pervasive Computing field.

For the NIST Aroma project, we have developed the Layered Pervasive Computing model, where users are considered as key elements of pervasive computing. We are also developing EXiST, the Experimental Simulation Tool. It is being created to explore pervasive computing requirements and use cases with the ultimate goal of using a case-based approach to defining this field. Artificial Intelligence will be part of this new world, and we are currently exploring the use of Intelligent Agents. They can learn or even teach how to use resources by interacting with human users, providing a higher level of intelligence to the environment, but they also can be used as human models in simulations or in expert systems. We are using COGNET, a cognitive agent modeling toolkit in conjunction with EXiST to create “unit” agents to help define usability metrics in pervasive computing.

Coakley, K.J., Chen-Mayer, H.H., Lamaze, G.P., Simons, D.S., Thompson, P.E.	Calibration of a Stopping Power Model for Silicon Based on Analysis of Neutron Depth Profiling and Secondary Ion Mass Spectrometry Measurements	Nuclear Instruments and Methods in Physics Research A
---	--	--

We measure the boron concentration versus depth profile within a silicon sample with four delta-doped planes by Secondary Ion Mass Spectrometry (SIMS). In a Neutron Depth Profiling (NDP) experiment, we illuminate the sample with a neutron beam. Nuclear reactions between the boron nuclei and neutrons produce alpha particles. Based on the measured boron concentration profile and models for the stopping power of the silicon sample, energy straggling, multiple scattering, and the observed energy resolution of the alpha particle detector, we predict the observed energy spectrum of the detected alpha particles. We predict the stopping power of silicon using the Transport of Ions in Matter (TRIM) code. The predicted locations of the NDP energy peaks are consistently at lower energies than the locations of the observed peaks. This discrepancy is consistent with the claim that TRIM overestimates the actual stopping power of silicon. Empirically, we estimate a stopping power reduction factor to be 5.06 +/- 0.35 percent. When we reduce the TRIM prediction by this factor, we get good agreement between the observed and

Coakley, K.J., Levenson, M.S.	Commentary for Special Issue on Quantitative Imaging	International Journal of Imaging Systems and Technology
-------------------------------	---	--

Kevin Coakley and Mark Levenson were invited to solicit papers on Quantitative Imaging for a special issue of the International Journal of Imaging Systems and Technology. They briefly describe the papers in a commentary that will appear in the special

Author	Title	Place of Publication	Date
Coakley, K.J., Yang, G.L.	Background-Correction for Neutron Lifetime Experiments: Best Strategy?	Physical Review C	

In the first stage of each run of a neutron lifetime experiment, a magnetic trap is filled with neutrons. In the second stage of each run, neutron decay events plus background events are observed. In a separate experiment of multiple runs, only background signals are measured after refilling the trap. In one approach, the mean lifetime of the neutron is estimated by fitting a two-parameter exponential model to the background-corrected data. In a second approach, the neutron lifetime is estimated by fitting a more complicated model to the “neutron decay plus background” data and the “background only” data coming from both

Author	Title	Place of Publication	Date
Croarkin, M.C.	Statistics and Measurement	NIST Journal of Research, Vol. 106, No. 1, pp. 279-292, January-February 2001	1/31/2001

For more than 50 years, the Statistical Engineering Division (SED) has been instrumental in the success of a broad spectrum of metrology projects at NBS/NIST. This paper highlights fundamental contributions of NBS/NIST statisticians to statistics and to measurement science and technology. Published methods developed by SED staff, especially during the early years, endure as cornerstones of statistics not only in metrology and standards applications, but as data-analytic resources used across all disciplines. The history of statistics at NBS/NIST, began with the formation of what is now the SED. Examples from the first five decades of the SED illustrate the critical role of the division in the successful resolution of a few of the highly visible, and sometimes controversial, statistical studies of national importance. A review of the history of major early publications of the division on statistical methods, design of experiments, and error analysis and uncertainty is followed by a survey of several thematic areas. The accompanying examples illustrate the importance of SED in the history of statistics, measurements and standards: calibration and measurement assurance, interlaboratory tests, development of measurement methods, Standard Reference Materials, statistical computing, and dissemination of measurement technology. A brief look forward sketches the expanding opportunity and demand for SED statisticians created by current trends in research and development at NIST.

Cugini, J.V.	FORTTRAN Test Programs	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 258-259	1/31/2001
--------------	------------------------	---	-----------

Cugini, J.V.	The FLUD Format: Logging Usability Data from Web-Based Applications	NIST SP 500-247 (web only at http://www.itl.nist.gov/iaui/vvrg/cugini/webmet/flud/specification.html)	1/3/2001
--------------	---	--	----------

This paper presents a proposed format for representing the behavior of users as they interact with a web-based application. The captured log data can be valuable for analyzing and improving the usability of such applications. The background and motivation of this effort are briefly described. The detailed syntax and semantics of the format are then defined.

Cugini, J.V., Laskowski, S.J.	Design of a File Format for Logging Website Information	NIST SP 500-248 (web only at http://www.itl.nist.gov/iaui/vvrg/cugini/webmet/flud/design-paper.html)	4/11/2001
-------------------------------	---	--	-----------

The logging of user behavior in support of web usability testing is constrained by the difficulty of capturing and analyzing large amounts of logged data. However, there is great potential for the development of tools to support automated recording and

analysis, especially for remote or large scale testing. In this paper, we propose a format for the representation of user interaction with a website. A widely accepted format enables the development of a set of software tools to process the data, the sharing of data sets for longer term analysis and research, and provides a common language for expressing user interaction

Cypher, D.	What to Expect When You Cannot Start at the Beginning	Proceedings of the Telelogic's Americas' 2001 User Group Conference (UGC) Round-Up, 8th Annual User Group Conference, San Antonio, Texas, July 12-14,
------------	---	---

This presentation contains background information on the decision to create an Specification and Description Language (SDL) model, a discussion of the development cycle for the product development, a description of the SDL's creation, an explanation on how the SDLs are being used, a log of the types of problems encountered during this process, and a list of possible extensions to the SDL models and language. The purpose of this presentation is to show the drawbacks in not creating an SDL as part of a product's development cycle and some of the advantages to creating an SDL afterwards.

Author	Title	Place of Publication	Date
Dabrowski, C., Mills, K.	Analyzing Properties and Behavior of Service Discovery Protocols Using an Architecture-Based Approach	Proceedings of a Workshop on Architectures for Complex and Dynamic Systems	

Current trends suggest that future software components will need to discover and adapt to dynamic changes in available software services and network connections. This implies that future systems may appear as collections of components that combine and recombine dynamically in reaction to changing conditions. Such environments demand new analysis approaches and tools for software design, implementation, and testing. Our work considers how one might rigorously assess the robustness of distributed software systems in response to dynamic change, such as process, node, and link failures. More particularly we seek techniques that can be applied early in the development process to test the behavior and resilience of dynamic distributed systems, and to compare and contrast various approaches to design such systems. As a challenging application we investigate service discovery protocols. We adopt an architecture-based approach that entails the following general steps: (1) construct an architectural model of each discovery protocol, (2) identify and specify relevant consistency conditions that each model should satisfy, (3) define appropriate metrics for comparing the behavior of each model, (4) construct interesting scenarios to exercise the models and to probe for violations of consistency conditions, and (5) compare the results from executing similar scenarios against each model. We elaborate our approach, using Jini as a specific example, and show how Jini can be analyzed using Rapide, an Architecture Description Language (ADL). Our analyses take two forms: property analysis and event analysis. Both depend upon Rapide's ability to execute a specification and to generate events. We use property analysis to investigate robustness to dynamic change, while we use event analysis to discern underlying causes of observed behavior and performance. We argue that static, natural-language specifications largely miss collective behavior arising when various components interact together in a distributed system. We show that a single architectural model can be used to understand both

logical and performance properties of a distributed system design. We evaluate how well Rapide supported our modeling and analyses. We also recommend improvements in ADLs to help test and analyze designs for distributed systems.

Dabrowski, C.E.	Characteristics of ADLs That Support Good Architecture Documentation: A Position Paper for the SEI Software Architecture Workshop	Proceedings of Software Engineering Documentation Workshop, January 16-17, 2001	1/16/2001
-----------------	---	---	-----------

One of the potential benefits of describing software architecture is the ability to provide greater clarity and understanding than what is possible in program code. The concise representation of the essential aspects of the functional components of a system, their connections and interactions, and their behavior provides a basis for communicating system design. This serves as documentation for different stakeholders and participants in the system design process, including system analysts, designers, implementers, maintainers, and managers. In current software practice, the development of comprehensive documentation of any aspect of a system--including its architecture--is often lengthy and tedious. This is particularly the case when describing a system using a terminology familiar to customers or when it is necessary to provide alternative views of a system to different stakeholders. To provide the greatest benefit with the least amount of effort, it should be possible for an architecture description to be stated completely in a specification created using the ADL. That is, a specification written in an ADL should be as self-documenting as possible. While additional text will always be required to provide context and design rationale, the actual specification of software architecture in the ADL should be definitive enough not to require large amounts of additional explanation and comments. This position paper makes recommendations on good characteristics of architecture documentation and discusses ADL features that support such characteristics.

Author	Title	Place of Publication	Date
Davies, M. A., Pratt, J. R., Dutterer, B., Burns, T. J.	Regenerative Stability Analysis of Highly Interrupted Machining	Accepted by Metal Cutting and High Speed Machining, D. Dudzinski, et al., eds., Kluwer Academic/Plenum Publishers	

We discuss theoretical and experimental work that supports the use of very low radial immersion in the high-speed milling of difficult-to-machine materials, such as titanium alloys. Our theory is based upon modeling the cutting process by a kicked harmonic oscillator with delay. Traditional regenerative chatter theory predicts that, for a single degree of freedom system, the most stable speeds are at integral multiples of the natural frequency of the system. The new theory predicts a set of stable speeds at fractions of the damped natural frequency. For small damping, a subset of these stable speeds is approximately the same as predicted by the traditional theory. From a practical point of view, the most important prediction of our new theory is that the number of optimally stable speeds doubles as the ratio r of time per revolution of tool contact with the material to the spindle period becomes small, i.e. $r \ll 1$. Co-authors on this work are M.A. Davies, J.R. Pratt, and B. Dutterer of the NIST

Devaney J.E., Hagedorn, J.G., Nicolas, O.P., Garg, G., Samson, A., Michel, M.	A Genetic Programming Ecosystem	Proceedings of the 15th Annual International Parallel and Distributed Processing Symposium, IPDPS 2001, Workshop on Biologically Inspired Solutions to Parallel Processing Problems	4/23/2001
---	---------------------------------	--	-----------

Algorithms are needed in every aspect of parallel computing. Genetic Programming is an evolutionary technique for automating the design of algorithms through iterative steps of mutation and crossover operations on an initial population of randomly generated computer programs. This paper describes a parallel genetic programming (GP) system inspired by the symbiogenesis model of evolution, wherein new organisms are generated through the absorption of different life-forms in addition to the usual mutation and crossover operations. Different organisms are expressed in this GP system through multiple program representations. Two program representations considered in this paper are the procedural representation (PR) and the tree representation (TR). Populations of these representations evolve separately. Individuals in each population migrate to the other and participate in evolution via representation change algorithms. Parallelism is achieved through use of the AutoMap/AutoLink MPI library. The differences in the locality properties of the representations serve as a source of new ideas for creating the final

Dienstfrey, A., Greengard, L.	Analytic Continuation, Singular Value Expansions, and Kramers-Kronig	Accepted by Inverse Problems	3/30/2001
-------------------------------	---	------------------------------	-----------

We describe a systematic approach to the recovery of a function analytic in the upper half plane, \mathbb{C}^+ , from measurements over a finite interval on the real axis, $D \subset \mathbb{R}$. Analytic continuation problems of this type are well-known to be ill-posed. Thus, the best one can hope for is a simple, linear procedure which exposes this underlying difficulty and solves the problem in a least squares sense. To accomplish this, we first construct an explicit analytic approximation of the desired function and recast the continuation problem in terms of a "residual function" defined on the measurement window D itself. The resulting procedure is robust in the presence of noise and we demonstrate its performance with some numerical

Dima, A.A., Ciarletta, L.P.	The Case for Simulation-Based Evaluation of Ubiquitous Computing Environments	UbiComp01 Workshop on Evaluation Methodologies for Ubiquitous Computing
-----------------------------	---	---

Ubiquitous computing (a.k.a. pervasive computing) is ill-defined due to its novelty and the community's current emphasis on its technological aspects. This can lead to serious "existential" issues during the evaluation of ubiquitous computing technologies.

Use-case driven simulations can address these issues by providing a context for the analysis of ubiquitous computing

Author	Title	Place of Publication	Date
Duff, I., Herous, M., Pozo, R.	"The Sparse BLAS" Technical Report	Rutherford Appleton Laboratory RAL-TR-2001-032, August 2001	8/1/2001
<p>We discuss the interface design for the Sparse Basic Linear Algebra Subprograms (BLAS), the kernels in the recent standard from the BLAS Technical Forum that are concerned with unstructured sparse matrices. The motivation for such a standards to encourage portable programming while allowing for library-specific optimizations. In particular, we show how this interface can shield one from concern over the specific storage scheme for the sparse matrix. This design makes it easy to add further functionality to the sparse BLAS in the future. We illustrate the use of the Sparse BLAS with examples in the three supported programming languages, Fortran 95, Fortran 77, and C.</p>			
Dworkin, M.	Conference Report: Third Advanced Encryption Standard Candidate Conference	Web (http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm)	7/25/2001
<p>On April 13-14, 2000, over two hundred members of the global cryptographic research community attended the Third Advanced Encryption Standard Candidate Conference, in New York, NY. At this point in NIST's effort to develop the AES, there were five finalist algorithms under consideration. The main purpose of the conference was to advise NIST in the selection of one or more of the five finalist candidate algorithms for inclusion in the AES. The presentations of papers were organized into the following sessions: field programmable gate array (FPGA) evaluations, platform-specific evaluations, survey evaluations, cryptographic properties and analysis, application specific integrated circuit (ASIC) evaluations, and recent results. In addition there were panel sessions devoted to AES issues and to algorithm submitter presentations, followed by audience questions and discussion.</p>			
Eggleston, J. J., McFadden, G. B., Voorhees, P. W.	A Phase-Field Model for Highly Anisotropic Interfacial Energy	NISTIR 6706 and Physica D	1/15/2001
<p>A computationally efficient phase-field model is developed for two-phase systems with anisotropic interfacial energy. The approach allows for anisotropies sufficiently high that the interface has corners or missing crystallographic orientations. The method employs a regularization that enforces local equilibrium at the corners and allows corners to be added or removed without explicitly tracking their location. Numerical simulations for various degrees of anisotropy were performed and they show excellent agreement with analytical equilibrium shapes and yield accurate time dependent solutions for a wide variety of initial</p>			

Fenimore, C., Floyd, M.

Digital Cinema 2001 Conference
Proceedings

NISTIR 6591

1/11/2001

This Proceeding provides papers and slides for the presentations at digital Cinema 2001 Conference. The conference addresses a variety of business and technical issues arising in developing digital cinema. Speakers address: on overview of digital cinema, studio and theater owners perspectives, compression, standards, measurement of projected image quality, digital rights management, storage and other topics.

Fenimore, C., Nikolaev, A.I.

Software for Viewing and Converting
Digital Cinema Materials

NISTIR 6814

Digital cinema (d-cinema) is the highest quality electronic motion imagery for entertainment. The cinema is presented in a theatrical environment, with high brightness projectors, high rate data transfer, and high resolution color imagery. The entertainment industry uses formats that are specific to film-based electronic imagery and there is a need for software tools to generate and manipulate test patterns for d-cinema systems. This report describes the principal software interfaces used to generate and view test imagery in connection with recent d-cinema system tests. The tools, which support the d-cinema quality measurement needs of the movie industry, are available on line.

Author

Title

Place of Publication

Date

Fiscus, J.G., Doddington, G.R.

Topic Detection and Tracking
Evaluation Overview

Topic Detection and Tracking:
Event-Based Information
Organization Editors: James Allan,
Jaime Carbonell, Jonathan Yamron

The objective of the Topic Detection and Tracking (TDT) program is to develop technologies that search, organize and structure multilingual, news oriented textual materials from a variety of broadcast news media. This research program uses controlled laboratory simulations of hypothetical systems to test the efficacy of potential technologies, to gauge research progress, and to provide a forum for the exchange of research information. This chapter introduces TDT's evaluation methodology including: the Linguistic Data Consortium's TDT corpora, evaluation metrics used in TDT and the five TDT research tasks: Topic Tracking, Link Detection, Topic Detection, First Story Detection, and Story Segmentation.

Fiscus, J.G., Doddington, G.R.

Results of the 1999 Topic Detection
and Tracking Evaluation in Mandarin

6th International Conference on
Spoken Language Processing

and English

(ICSLP) Beijing, China

The National Institute of Standards and Technology (NIST) administered the second open evaluation of Topic Detection and Tracking (TDT) technologies in 1999. The TDT project supports development of technologies that automatically organize event-related news stories. The program leverages expertise in core technologies, Automatic Speech Recognition (ASR), Document Retrieval (DR), and Machine Translation (MT) to build the TDT technologies. The 1999 TDT project extended the 1998 TDT project in two dimensions, first by adding Mandarin Chinese audio and text sources and second by adding two new evaluation tasks. Through experimental controls and conditioned analysis of system performance, the 1999 evaluation yielded numerous insights into the effects of multilingual texts on TDT technologies. Three notable generalizations arise from the evaluation: (1) English and Mandarin story segmentation performance is similar, (2) cross-lingual topic tracking performance is 44% worse than monolingual tracking, and (3) multilingual topic detection performance is 37% worse than monolingual topic

Fong, E. N., Ivezic, N., Rhodes, T.
R., Peng, Y.

Agent-Based Services for B2B
Electronic Commerce

Conference Proceedings of SPIE
(International Society for Optical
Engineering) – Session VV13

The potential of agent-based systems has not been realized yet, in part, because of the lack of understanding how the agent technology support industrial needs and emerging standards. The area of business-to-business electronic commerce (b2b e-commerce) is one of the most rapidly developing sectors of industry with huge impact on manufacturing practices. Our intent in this paper is to investigate the current state of agent technology and the feasibility of applying agent-based computing to b2b e-commerce in the circuit board manufacturing sector. We identify critical tasks and opportunities in the b2b e-commerce area where agent-based services can best be deployed. We describe an implemented agent-based system to facilitate the bidding process for printed circuit board manufacturing and assembly. These activities are taking place within the Internet Commerce for Manufacturing (ICM) project, the NIST-sponsored project working with industry to create an environment where small manufacturers of mechanical and electronic components may participate competitively in virtual enterprises that manufacture

Frankel, S.

An Introduction to IPsec (Internet
Protocol Security)

ITL Bulletin, March 2001

3/30/2001

IPsec (Internet Protocol Security) is an attempt to utilize cryptographic techniques in a global solution to the problem of Internet security. Rather than requiring each email program or Web browser to implement its own security mechanisms, IPsec involves a change to the underlying networking facilities that are used by every application. It also allows network managers to apply protection to network traffic without involving the end users. This security bulletin discusses the types of protection provided by IPsec, its major components, current uses, and future potential.

Author	Title	Place of Publication	Date
Gallagher, L.J., Offutt, A.J.	Integration Testing of Object-Oriented Components Using Finite State	Software Testing, Verification and Reliability Wiley Inter Science, John Wiley & Sons, Ltd.	

In object-oriented terms, integration testing tries to ensure that messages from objects in one class or component are sent and received in the proper order and have the intended effect on the state of external objects that receive the messages. This research focuses on integration testing. It is based on work by Hong, Kwon, and Cha, who model the behavior of a single class as a finite state machine, transform that representation into a data flow graph that explicitly identifies the definitions and uses of each state variable of the class, and then apply conventional data flow testing to produce test case specifications that can be used to test conformance of the given class to its functional specification. This paper extends those ideas to inter-class testing by developing flow graphs and tests for an arbitrary number of classes and components. It introduces flexible representations for message sending and receiving among objects and allows parallel processing among any or all classes and components. A second major result is the introduction of a novel approach to performing data flow analysis. Data flow graphs are stored in a relational database, and SQL queries are used to gather def-use information. This approach is conceptually simple, mathematically precise, quite powerful, and general enough to be used for traditional data flow analysis. Our testing approach relies on finite state machines, database modeling and processing techniques, and algorithms for analysis and traversal of directed graphs. A proof-of-concept implementation of the approach demonstrates its effectiveness on an industrial application.

Galtier, V., Mills, K., Carlinet, Y., Bush, S.	Predicting Resource Demand in Heterogeneous Active Networks	MILCOM 2001 Conference	10/30/2001
--	---	------------------------	------------

Recent research, such as the Active Virtual Network Management Prediction (AVNMP) system, aims to use simulation models running ahead of real time to predict resource demand among network nodes. If accurate, such predictions can be used to allocate network capacity and to estimate quality of service. Future deployment of active-network technology promises to complicate prediction algorithms because each “active” message can convey its own processing logic, which introduces variable demand for processor (CPU) cycles. This paper describes a means to augment AVNMP, which predicts message load among active-network nodes, with adaptive models that can predict the CPU time required for each “active” message at any active-network node. Typical CPU models cannot adapt to heterogeneity among nodes. This paper shows improvement in AVNMP performance when adaptive CPU models replace more traditional non-adaptive CPU models. Incorporating adaptive CPU models can enable AVNMP to predict active-network resource usage farther into the future, and lowers prediction overhead.

Galtier, V., Mills, K., Carlinet, Y., Bush, S., Kulkarni, A.	Predicting and Controlling Resource Usage in a Heterogeneous Active	Proceedings 3rd International Workshop on Active Middleware Systems	
--	---	---	--

Active network technology envisions deployment of virtual execution environments within network elements, such as switches and routers. As a result, inhomogeneous processing can be applied to network traffic. To use such technology safely and efficiently, individual nodes must provide mechanisms to enforce resource limits. This implies that each node must understand the varying resource requirements for specific network traffic. This paper presents an approach to model the CPU time requirements of active applications in a form that can be interpreted among heterogeneous nodes. Further, the paper demonstrates how this approach can be used successfully to control resources consumed at an active-network node and to

predict load among nodes in an active network, when integrated within the Active Virtual Network Management Prediction

Author	Title	Place of Publication	Date
Garris, M.D.	Latent Fingerprint Training with NIST Special Database 27 and Universal Latent Workstation	NISTIR 6799	9/30/2001

The National Institute of Standards and Technology, in collaboration with the FBI, has published NIST Special Database 27 (SD27) "Fingerprint Minutiae from Latent and Matching Tenprint Images." This CD-ROM collection contains images of 258 latent crime scene fingerprints and their matching rolled tenprints. In addition, minutiae features validated by a team of professional latent examiners are provided for each fingerprint. Meanwhile, the FBI has also developed the Universal Latent Workstation (ULW). This workstation has been designed to render and enhance fingerprint images, assist the operator in labeling minutiae and other fingerprint features, and formatting this information into a standard transaction file for searching federal, state, and local law enforcement fingerprint repositories. Using the ULW in conjunction with SD27 poses a powerful and inexpensive training tool for fingerprint examiners. This report documents the steps needed to load SD27 fingerprint images into ULW, and how trainee results can then be overlaid with the validated minutiae in SD27. Given these steps, a variety of training scenarios are possible.

Garris, M.D., Watson, C.I., McCabe, R.M., Wilson, C.L.	User's Guide to NIST Fingerprint Image Software	NISTIR 6813	11/1/2001
--	---	-------------	-----------

This report documents a public domain fingerprint image software distribution developed by the National Institute of Standards and Technology (NIST) for the Federal Bureau of Investigation (FBI). The software technology contained in this distribution is a culmination of a decade's worth of work for the FBI at NIST. Provided are a collection of application programs, utilities, and source code libraries. These are organized into four major packages: 1. PCASYS is a neural network based fingerprint pattern classification system; 2. MINDTCT is a fingerprint minutiae detector; 3. AN2K is a reference implementation of the ANSI/NIST-ITL1-2000 "Data Format for the Interchange of Fingerprint, Facial, Scar Mark & Tattoo (SMT) Information" standard;

and 4. IMGTOOLS is a collection of image utilities, including encoders and decoders for Baseline and Lossless JPEG and the FBI's WSQ specification. This public domain source code distribution is written in 'C', and has been developed to compile and execute under the Linux operating system using the GNU gcc compiler and make utility. The source code may also be installed to run on Win32 platforms that have the Cygwin library and associated tools installed. A Reference Manual describing each

George, W.L., Hagedorn, J.G., Parallel Programming with Interoperable Accepted by Dr. Dobb's Journal
Devaney, J.E. MPI

In this article we describe IMPI (Interoperable Message Passing Interface), a message passing protocol that allows you to easily run parallel programs across multiple clusters, SMPs (symmetric multiprocessors), parallel machines, personal computers, and workstations, all with varying architectures and operating systems. IMPI is an extension to MPI (Message Passing Interface), the commonly used message passing library used for parallel scientific computing.

George, W.L., Warren, J. A Parallel 3D Dendritic Growth Submitted to Journal of
Simulator Using the Phase-Field Method Computational Physics

We describe a parallel implementation of an algorithm for the simulation of alloy solidification in three dimensions and the visualization of its output. Although this type of simulation has been accomplished before in two dimensions, extending this to three dimensions presents scaling problems for both the computations and the subsequent rendering of the results for visualization. This is due to the $O(n^4)$ execution time of the simulation algorithm as well as the $O(n^3)$ space requirements for holding the required three dimensional arrays of field parameters. Additionally, rendering the output of the three dimensional simulation also stresses the available software and hardware when the simulations extend over finite-difference grids of size 1000x1000x1000. Parallel computing and hardware supported rendering combine to help make this simulation possible.

Author	Title	Place of Publication	Date
Gérardin, O., Le Gall, H. Donahue, M. J., Vukadinovic, N.	Micromagnetic Calculation of the High Frequency Dynamics of Nano-Size Rectangular Ferromagnetic Stripes	Journal of Applied Physics 89 (2001), pp. 7012-7014	

Nano-size ferromagnetic dots, wires and stripes are of strong interest for future high speed magnetic sensors and ultra high density magnetic storage. High frequency dynamic excitation is one way to investigate the time scale of the magnetization

reversal in submicron particles with lateral nanometer dimension. Macroscopic models like the Landau-Lifshitz (LL) model are often used to describe the switching process. However, these models do not take into account the non-uniformity of the magnetization structure. In this paper dynamic micromagnetic calculations are used in determining the high frequency susceptibility of a 1 μm x 50 nm x 5 nm permalloy stripe. The studied structure exhibits two resonance modes. The higher, primary peak is around 10 GHz, and can be identified with the uniform resonance mode predicted by the macroscopic LL model. The low frequency peak is attributed to the divergence of the magnetization distribution near the end of the stripe.

Gharavi, H., Wyatt-Millington, R., Chin, F. Design, Model Implementation, and Evaluations of the CDMA2000 Reverse-Link NIST Journal of Research and Milcom 2001, McLean, Virginia, October 28-31, 2001 10/28/2001

cdma-2000 service is the evolutionary enhancement of the IS-95A, and IS-95B standards to support 3G services defined by the International Telecommunications Union (ITU). cdma2000 comes in two phases. The first is cdma2000 1XRTT that operates within a 1.25 MHz bandwidth and thus, can be used in existing cdma channels as it uses the same bandwidth. The second phase is 3XRTT, which requires a 5MHz spectrum commitment for both the forward and reverse links. The 1X and 3X refer to the number of 1.25 MHz wide radio carrier channels used, and RTT refers to radio-transmission technology. This report presents a design and implementation procedure for a simulation model of the cdma2000 reverse link. The reverse link has been implemented at the National Institute of Standards and Technology (NIST), using Signal Processing WorkSystem (SPW) software simulation tools developed by Cadence Design System Inc. The model has been developed in a generic manner that includes all the reverse link six radio configurations and their corresponding data rates according to the IS-2000 specifications. For performance evaluations and measurements, a sophisticated link budget has also been implemented in accordance with IS-2000 specifications. The report, after providing a tutorial review of the reverse link characteristics and its SPW implementation, presents the results of our measurement and performance evaluations when transmitted over imt2000 fading channels.

Gharavi, H., Wyatt-Millington, R., Chin, F. CDMA2000 Reverse-Link Simulation Model Design and Evaluation NIST Journal of Research and 2001 International Conference on Third Generation Wireless and Beyond, San Francisco, California, May 30–June 2, 2001

This paper presents the design and implementation of a simulation model for the cdma2000 reverse link. The model includes all the radio configurations and their corresponding data rates in accordance with the IS-2000 specifications. The paper first presents a tutorial review of the traffic channel characteristics of the cdma2000 reverse link (subscriber to base station) and its physical layer performance by considered two types of rake receivers; ideal and non-ideal. The reverse link performance is measured based on its link budget specifications.

Gilsinn, D.E. Machine Tool Chatter: A Genuine Hopf Bifurcation Nonlinear Dynamics

Regenerative machine tool chatter is modeled as a delay differential equation. The equation is shown to satisfy all the hypotheses of the Hopf Bifurcation Theorem by using multiple techniques. A graphical based method is used to construct the stability boundaries satisfied by the solutions of the characteristic equation along the positive imaginary axis. Implicit function

techniques are used to prove the existence of a family of solutions satisfying the transversality condition at the boundary. Contour integration is used to show that all eigenvalues except the unique conjugate pair on the imaginary axis have negative real parts. Several cases are simulated in order to show the Hopf bifurcation occurring at the stability boundary. A discussion of

Author	Title	Place of Publication	Date
Gilsinn, D.E.	Constructing Sibson Elements for a Rectangular Mesh	NISTIR 6718	2/28/2001

This paper documents the construction of a finite element, called the Sibson element. The shape function of this element is formed on rectangular grids by splines defined on a triangulation of each subrectangle by dividing it into four subtriangles formed by drawing the diagonals. The splines are constructed from bivariate cubic polynomials and are written in such a way that they are linear functions of the z, at each node of the rectangle with bivariate polynomial coefficients up to order three. Conditions are given for the existence of such an element. They are used to construct the bivariate polynomial coefficients, first for a unit rectangle and then for a general rectangle. Since the first and second derivatives of these functions are

Gilsinn, D.E., Bandy, H.T., Ling,	Updating a Turning Center Error Model by Singular Value Decomposition	NISTIR 6722	3/15/2001
-----------------------------------	---	-------------	-----------

The precision of manufacturing using machine tools depends on the accuracy of the relative position of the cutting tool with respect to the workpiece. Kinematic modeling of machine tools is used to describe this relative position. This motion can be modeled by homogeneous coordinate transformation matrices composed of both rotational elements as well as positional offset elements of the associated coordinates. The rotation and translation components of the homogeneous are considered to be functions of nominal tool position and machine temperatures. In general these functions are low order polynomials in terms of position and temperatures. The coefficients are usually calculated with least squares curve fitting techniques. The data for these fits are obtained by measuring actual coordinate positions and temperatures on the machine tool based upon desired programmed nominal coordinates. The process of measuring and modeling the errors of machine axis positions as functions of nominal positions and temperatures is referred to as machine tool characterization. The geometric-thermal models developed through machine tool characterization may not fully predict the errors encountered by a machine tool during machining. The data from machine characterization usually provides the structure to derive the basic form of the equations used to model the various error components used in the homogeneous matrices. This process of model updating involves determining the residual systematic errors of the machine tool and applying an algorithm to update the geometric-thermal model coefficients. The updating algorithm described in this report begins with adding perturbation terms to the characterization coefficients of the geometric-thermal model. These coefficients are estimated by an "inverse" process, using residual systematic errors, determined from part measurements on a coordinate measuring machine. The main tool used in identifying the perturbation terms is called a generalized or pseudo inverse matrix. This matrix is applied to the residual error vector to obtain a "best"

Gilsinn, D.E., Lavery, J.E.	Shape-Preserving, Multi-Scale Fitting of	Submitted to Proceedings of	
-----------------------------	--	-----------------------------	--

Bivariate Data by Cubic L1 Smoothing Splines

Approximation Theory X

Bivariate cubic L1 smoothing splines are introduced. The coefficients of a cubic L1 smoothing spline are calculated by minimizing the weighted sum of the L1 norms of second derivatives of the spline and the l1 norm of the residuals of the data-fitting equations. Cubic L1 smoothing splines are compared with conventional cubic smoothing splines based on the L2 and l2 norms. Computational results for fitting a challenging data set consisting of discontinuously connected flat and quadratic areas by C1-smooth Sibson-element splines on a tensor-product grid are presented. In these computational results, the cubic L1 smoothing splines preserve the shape of the data while cubic L2 smoothing splines do not.

Golmie, N., Van Dyck, R.E.,
Soltanian, A., El Bakkouri, I.

Performance Evaluation of Bluetooth
and IEEE 802.11 Devices Operating in
the 2.4 GHz ISM Band

Proceedings of the 7th Annual
International Conference on Mobile
Computing and Networking
(MobiCom) 2001, Rome, Italy, July
16-21, 2001

The emergence of several radio technologies such as Bluetooth, and IEEE 802.11 operating in the 2.4 GHz unlicensed ISM frequency band may lead to signal interference and result in significant performance degradation when devices are co-located in the same environment. The main goal of this paper is to present a performance evaluation of these radio systems sharing the same air space based on an integrated MAC and PHY simulation model. Our results focus on the impact of interference on Bluetooth and IEEE 802.11. We use several simulation scenarios and measure performance in terms of packet loss, residual

Author	Title	Place of Publication	Date
Gray, M.M.	Code for Information Interchange	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 172-173.	1/31/2001
Grother, P., Casasent, D.	New MTF Measurement Method for Electrically Addressed SLMs	Applied Optics	

The modulation transfer function (MTF) using amplitude modulation (mA) data is a vital coherent optical performance measure for a spatial light modulator (SLM). A new image plane MTFA (amplitude MTF) measurement method is presented for electrically addressed SLMs. It involves digital analysis of the output image of a square-wave pattern written onto the SLM. Modulation level effects are also addressed. Optical laboratory results are presented for two liquid crystal SLMs. The need to consider

amplitude not intensity modulation (when coherent optical processing applications are considered) is noted in terms of SLM

Gurski, K.F.	Hints for Finding Non-Academic Research Positions (Postdoctoral and	Association for Women in Mathematics Newsletter, September-October 2001, pp. 17-19	10/1/2001
--------------	---	--	-----------

Gurski, K.F.	An HLLC-Type Approximate Riemann Solver for Ideal	Journal of Computational Physics
--------------	---	----------------------------------

This paper presents a new solver based on the HLLC (Harten-Lax-van Leer-contact wave) approximate nonlinear Riemann solver for gas dynamics for the ideal magnetohydrodynamics (MHD) equations written in conservation form. It is shown how this solver also can be considered a modification of Linde's "Adequate" solver. This approximation method is intended to be less diffusive for all problems containing contact waves than the HLL solver. Compared to exact nonlinear solvers and Roe's solver, this new solver is computationally inexpensive. In addition, the method will exactly resolve isolated shocks and contacts. The method also is guaranteed to preserve positive density and pressure although in a few cases positivity may require changing the wavespeeds of the Riemann fan for the underlying HLL method. While the method is intended for a three-dimensional MHD problem, the simulation results concentrate on one-dimensional test cases.

Gurski, K.F., Pego, R.L.	Normal Modes for a Stratified Viscous Fluid Layer	Accepted by Proceedings of the Royal Society of Edinburgh A
--------------------------	---	---

We consider internal gravity waves in a stratified fluid layer with rigid horizontal boundaries and periodic boundary conditions on the sides at constant temperature with a small constant viscosity, modeled using the incompressible Navier-Stokes equations. Using operator-theoretic methods to study the damping rates of internal waves, we prove there are non-oscillatory wave modes with arbitrarily small damping rates. We provide an asymptotic approximation for these non-oscillatory modes. Additionally we find that the eigenvalues for damped oscillations are in an explicitly describable half ring.

Author	Title	Place of Publication	Date
Guthrie, W.F.	Should (T1- T2) Have Larger Uncertainty Than T1?	Proceedings of the 8th International Symposium on Temperature and Thermal Measurements in Industry and Science	

In interlaboratory comparisons, laboratories sometimes use a transfer instrument to realize the value of a laboratory standard to compare the relative biases of their measurement processes and standards. One summary of interest from such comparisons is the pairwise difference between two laboratories' results, along with its expanded uncertainty, a confidence interval for the true difference. Since the labs have unequal variances, the confidence interval is usually computed by the Welch-Satterthwaite (denoted WS) procedure, which approximates the distribution of the pivot quantity used to compute the confidence interval by a Student's-t distribution with effective degrees of freedom defined as a function of the data. In the course of analyzing the data from a comparison of temperature realizations, an awkward and counterintuitive property of the WS procedure was observed. Namely, a confidence interval for a between-lab difference can be narrower than the corresponding interval for one of the component results. This occurs when at least one laboratory's uncertainty estimate has low degrees of freedom (say 1 or 2), and therefore has a large coverage factor from the Student's-t distribution, while the effective degrees of freedom for the combined uncertainty of the pairwise difference, obtained from the WS approximation, is larger. The typical reaction to this situation is to suspect the WS procedure of failing to achieve its nominal confidence level. However, this is not the correct explanation. In fact, situations exist where the confidence intervals for each laboratory's mean and for their pairwise difference all achieve the stated level of confidence even though the uncertainty of the difference is smaller than the uncertainty of at least one of its component results. This paper explains how this counterintuitive property of confidence intervals can be true.

Hagedorn, J.G., Devaney, J.E.	A Genetic Programming System with a Procedural Program Representation	Proceedings of the Late Breaking Papers in Genetic and Evolutionary Computation Conference 2001 (GECCO), San Francisco, California, July 7-11, 2001, pp.	7/7/2001
-------------------------------	---	--	----------

We describe the status of a genetic programming system that is based on a procedural program representation. The procedural representation is closely related to the high level programming languages used by human programmers; it includes features such as hierarchies of procedure calls, with arguments lists that allow multiple output values from each procedure. This representation is structurally different than previous representations used in GP and is expected to have different evolutionary properties. The system architecture is presented and specific benefits as well as problems and solutions arising from this program representation are described. Two mutation-like operations, repair and pruning, are introduced. A population visualization technique is described that includes the graphical presentation of program structure, ancestry, and fitness. This visualization tool and other system instrumentation are used to investigate population diversity and fitness evolution. An

Hall, T.A.	Objective Speech Quality Measures for Internet Telephony	ITCom+OptiComm 2001, Denver, CO. August 19-24, 2001	
------------	--	---	--

Measuring voice quality for telephony is not a new problem. However, packet-switched, best-effort networks such as the

Internet present significant new challenges for the delivery of real-time voice traffic. Unlike the circuit-switched PSTN, Internet protocol (IP) networks guarantee neither sufficient bandwidth for the voice traffic nor a constant, minimal delay. Dropped packets and varying delays introduce distortions not found in traditional telephony. In addition, if a low bitrate codec is used in voice over IP (VoIP) to achieve a high compression ratio, the original waveform can be significantly distorted. These new potential sources of signal distortion present significant challenges for objectively measuring speech quality. Measurement techniques designed for the PSTN may not perform well in VoIP environments. Our objective is to find a speech quality metric that accurately predicts subjective human perception under the conditions present in VoIP systems. To do this, we compared three types of measures: perceptually weighted distortion measures such as enhanced modified Bark spectral distance (EMBSD) and measuring normalizing blocks (MNB), word-error rates of continuous speech recognizers, and the ITU E-model. We tested the performance of these measures under conditions typical of a VoIP system. We found that the E-model had the highest correlation with mean opinion scores (MOS). The E-model is well suited for online monitoring because it does not use the original (undistorted) signal to compute its quality metric and because it is computationally simple.

Author	Title	Place of Publication	Date
Harman, D., Braschler, M., Hess, M., Kluck, M., Peters, C., Schauble, P., Sheridan, P.	CLIR Evaluation at TREC	Proceedings of the Cross-Language Evaluation Forum Springer – Lecture Notes in Computer Science	
Starting in 1997, the National Institute of Standards and Technology conducted 3 years of evaluation of cross-language information retrieval systems in the Text REtrieval Conference (TREC). Twenty-two participating systems used topics (test questions) in one language to retrieve documents written in English, French, German, and Italian. A large-scale multilingual test collection has been built and a new technique for building such a collection in a distributed manner was devised.			
Heckert, A., Filliben, J.	NIST/SEMATECH Engineering Statistics Handbook, Chapter 1: Exploratory Data Analysis	Web	
This chapter presents an approach/philosophy for data analysis which employs a variety of techniques (mostly graphical) to: maximize insight into a data set; uncover underlying structure; detect outliers and anomalies; test underlying assumptions; and develop parsimonious models. The chapter also includes many case studies that show how to check a dataset for underlying			
Hersch, W., Over, P.	TREC-9 Interactive Track Report	Included in NIST SP 500-249	10/1/2001
The TREC-9 Interactive Track has the goal of investigating interactive information retrieval by examining the process as well as the results. In TREC-9, six research groups ran a total of 12 interactive information retrieval (IR) system variants on a shared problem: a fact-finding task, eight questions, and newspaper/newswire documents from the TREC collections. This report summarizes the shared experimental framework, which for TREC-9 was designed to support analysis and comparison of system			

performance only within sites. The report refers the reader to separate discussions of the experiments performed by each participating group – their hypotheses, experimental systems and results. The papers from each of the participating groups and the raw and evaluated results are available via the TREC home page (trec.nist.gov).

<p>Hogan, M.D., Carnahan, L.J., Carpenter, R.J., Flater, D.W., Fowler, J.E., Frechette, S.P., Gray, M.M., Johnson, L.A., McCabe R.M., Montgomery, D., Radack, S.M., Rosenthal, R., Shakarji, C.M.</p>	<p>Information Technology (IT) Measurement and Testing Activities at</p>	<p>NIST Journal of Research, Vol. 106, No. 1, January-February 2001</p>	<p>2/28/2001</p>
---	--	---	------------------

Our high technology society continues to rely more and more upon sophisticated measurements, technical standards, and associated testing activities. This was true for the industrial society of the 20th century and remains true for the information society of the 21st century. Over the last half of the 20th century, information technology (IT) has been a powerful agent of change in almost every sector of the economy. The complexity and rapidly changing nature of IT have presented unique technical challenges to NIST and to the scientific measurement community in developing a sound measurement and testing infrastructure for IT. This measurement and testing infrastructure for the important non-physical and non-chemical properties associated with complex IT systems is still in an early stage of development. This paper explains key terms and concepts for IT metrology, briefly reviews the history of NBS/NIST in the field of IT, and reviews NIST's current capabilities and work in measurement and testing for IT. It concludes with a look at what is likely to occur in the field of IT over the next ten years and

<p>Hogan, M.D., Johnson, L.A.</p>	<p>Data Management and Information Technology Requirements for Biomedical Materials and Devices</p>	<p>Included in NISTIR 6791</p>
-----------------------------------	---	--------------------------------

This paper is a summary of a workshop session during the Workshop on Biomedical Materials and Devices, held June 13 -14, 2001. The workshop is part of a series of workshops and topical meetings organized by NIST in the area of biomedical technology. The workshop complements other recent NIST efforts to make its leadership in standards and measurements more available to the health care industry, which accounts for about 13 % of the U.S. Gross National Product and continues to grow rapidly. This workshop session covered "Data Management and Information Technology Requirements."

Author	Title	Place of Publication	Date
<p>Jansen, W.A.</p>	<p>Intrusion Detection with Mobile Agents</p>	<p>Computer Communications Journal</p>	
<p>Implementing an effective intrusion detection capability is an elusive goal, not solved easily or with a single mechanism. However, we argue that mobile agent technology goes a long way toward realizing the ideal behavior desired in an Intrusion Detection System (IDS). This paper discusses various ways in which mobile agents could be applied to the problem of detecting and responding to intrusions. The paper looks not only at the benefits derived from mobility, but also at those associated with</p>			

software agents in general. After exploring these benefits, we outline a number of ways to apply mobile agent technology in addressing the shortcomings of current IDS designs and implementations. We also look at several new approaches for

Jansen, W.A. Guidelines on Active Content and Mobile Code NIST SP 800-28 (http://csrc.nist.gov/publications) 10/4/2001

The private and public sectors depend heavily upon information technology systems to perform essential, mission-critical functions. As new technologies are introduced and existing ones evolve to provide improved capabilities and advanced system features, new technology-related vulnerabilities often arise as well. Organizations implementing and using advanced technologies, therefore, must exercise caution. One such category of technologies is active content. Broadly speaking, active content refers to electronic documents that, unlike past American Standard Code for Information Interchange (ASCII) character documents, can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. Taken to its extreme, active content becomes, in effect, a delivery mechanism for mobile code. Therefore, exploits based on vulnerabilities in active content technologies by their very nature are often insidious. This document provides an overview of the subject and guidelines to Federal agencies for the protection of sensitive (i.e., non-national security) unclassified systems.

Jansen, W.A. Taming Active Content Canadian Information Technology Security Symposium

The private and public sectors depend heavily upon information technology (IT) systems to perform essential, mission-critical functions. As technology improves to provide new capabilities and features, new vulnerabilities are often introduced as well. Organizations implementing and using advanced technologies, therefore, must be increasingly on guard. One such emerging technology is active content. Although the term has different connotations among individuals, we use it here in its broadest sense to refer to electronic documents that, unlike ASCII character documents of the past, can carry out or trigger actions automatically without the intervention of a user. Examples of active content include PostScript documents, Java applets, JavaScript, word processing macros, spreadsheet formulas, and executable electronic mail attachments. Taken to its extreme, active content becomes, in effect, a delivery mechanism for mobile code. The purpose of this paper is to provide an overview of this topic and its underlying technologies, so that the reader becomes aware of the associated security risks and can make an informed IT security decision on its application. We review real-world examples involving commonly available products and

Jansen, W.A. A Privilege Management Scheme for Mobile Agent Systems Autonomous Agents Conference, SEMAS Workshop

In this paper, we describe a general method for controlling the behavior of mobile agent-system entities through allocation of privileges. Privileges refer to policy rules that govern the access and use of computational resources and services. The scheme is based on the capability of most mobile agent systems to extend the platform processing environment and the use of two forms of privilege management certificates: attribute certificates and policy certificates. Privilege management certificates are digitally signed objects that allow various policy setting principles to govern the activities of mobile agents through selective privilege assignment. This approach overcomes a number of problems in existing agent systems and provides a means for attaining improved interoperability of agent systems designed and implemented independently by different manufacturers. We

Author	Title	Place of Publication	Date
Kacker, R.N.	Towards a Simpler Bayesian Guide to the Expression of Uncertainty in	Proceedings of the Measurement Science Conference 2001	
<p>The impact of the Guide to Expression of Uncertainty in Measurement is spreading from the national measurement institutes to the industrial measurement laboratories. The Guide is written such that it can be loosely interpreted either from the frequentist or the Bayesian viewpoint. This paper presents a coherent interpretation of The Guide from a Bayesian viewpoint. This interpretation links The Guide with Bayesian statistics. This linkage should make the Guide more appealing to those interested in philosophical coherence. The Guide is not limited by the proposed interpretation. An immediate benefit of the Bayesian viewpoint is that it leads to a simpler and more reliable alternative to using a t-distribution with effective degrees of freedom as determined by Welch-Satterthwaite formula to account for a small number of measurements.</p>			
Kelso, J., Arsenault, L.E., Satterfield, S.G., Kriz, R.D.	DIVERSE: A Framework for Building Extensible and Reconfigurable Device Independent Virtual Environments	Proceedings of Virtual Reality 2002	
<p>We present DIVERSE, a highly modular collection of complimentary software packages designed to facilitate the creation of device independent virtual environments. DIVERSE is free/open source software; an API (Application Programming Interface) written in C++ and a collection of programs. DgiPf is the DIVERSE graphics to OpenGL Performer™. A program using DGIPf can run on platforms ranging from fully immersive systems such as CAVEs™ to generic desktop workstations without modification. We will describe DgiPf's design and present a specific example of how it is being used to aid researchers.</p>			
Ketcham, P.M., Feder, D.L., Clark, C.W., Satterfield, S.G., Griffin, T.J., George, W.L., Reinhardt, W.	Volume Visualization of Bose-Einstein Condensates	NISTIR 6739	4/30/2001
<p>An active area of research in the physics community is the study of Bose-Einstein condensation. Theoretical aspects of Bose-Einstein condensates are investigated by conducting computer simulations of their behavior. Scientific visualization techniques are employed in order to examine the large amount of data generated by simulation. Visualization of this simulated data demonstrates theoretical predictions, influences the research process, accelerates scientific understanding, and stimulates</p>			
Kirsch, R.A.	Computer Development at the National Bureau of Standards	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp.86-89.	1/31/2001
Kuhn, D.R.	A Hybrid Authentication Protocol Using	NISTIR 6741	

Quantum Entanglement and Symmetric
Cryptography

This paper presents a hybrid cryptographic protocol, using quantum and classical resources, for authentication and authorization in a network. One or more trusted servers distribute streams of entangled photons to individual resources that seek to communicate. It is assumed that each resource shares a previously distributed secret key with the trusted server, and that resources can communicate with the server using both classical and quantum channels. Resources do not share secret keys with each other, so that the key distribution problem for the network is reduced from n^2 to n . Some advantages of the protocol are that it avoids the requirement for timestamps used in classical protocols, guarantees that the trusted server cannot know the authentication key, can provide resistance to multiple photon attacks [Brassard et al., 1999; Felix et al., 2001] and can be used

Author	Title	Place of Publication	Date
Kuhn, D.R., Hu, V.C., Polk, W.T., Chang, S.J.	Introduction to Public Key Technology and the Federal PKI Infrastructure	NIST SP 800-32 (http://csrc.nist.gov/publications)	2/1/2001
This publication was developed to assist agency decision-makers in determining if a PKI is appropriate for their agency, and how PKI services can be deployed most effectively within a Federal agency. It is intended to provide an overview of PKI functions and their applications. Additional documentation will be required to fully analyze the costs and benefits of PKI systems for agency use, and to develop plans for their implementation. This document provides a starting point and references to more			
Langer, S.A., Carter, W.C., Fuller,	OOF: Image-Based Finite Element Analysis of Material Microstructure	IEEE Computing in Science and Engineering 3, no. 4, May-June 2001, p. 15	6/1/2001
The determination of macroscopic properties of a material given its microscopic structure is of fundamental importance to materials science. We present an overview of two public domain programs which jointly predict macroscopic behavior, starting from an image of the microstructure and ending with results from finite element calculations. The first program reads an image and assigns material properties to microscopic features. The second program reads the output of the first and performs virtual			
Lavery, J.E., Gilsinn, D.E.	Multiresolution Representation of Urban Terrain By L1 Splines, L2 Splines, and Piecewise Planar Surfaces	Proceedings 22nd Army Science Conference, Baltimore, Maryland, December 11-13, 2000, pp. 767-773	12/11/2000
Cubic L1 and L2 interpolating splines based on C1 smooth piecewise cubic Sibson elements on a tensor-product grid are investigated. Computational tests were carried out for an 800 m by 800 m area of Baltimore, MD represented by an 800 x 801			

set of 100-meter-spacing (posting) data set. Interpolating splines at coarser resolutions were computed along with I1, I2 and I?? errors relative to the 800 m by 800 m data set. Piecewise planar interpolations at the coarser resolutions were also computed along with the above errors for comparative purposes.

Lavery, J.E., Gilsinn, D.E.	Multiresolution Representation of Terrain By Cubic L1 Splines	Trends in Approximation Theory, (ed) Kirill Kopotun, Tom Lyche and Mike Neamtu, Vanderbilt Univ.
-----------------------------	---	--

Cubic L1 and L2 interpolating splines based on C1 smooth piecewise cubic Sibson elements on a tensor-product grid are investigated. Computational tests were carried out for a 102.4 km area of Fort Hood, Texas, represented by a 1025 x 1025 set of 100-meter-spacing (posting) DTED1 terrain data obtained from the National Imagery and Mapping Agency. L1 and L2 interpolating splines were calculated for this area using data at coarser spacings of 800 m, 1600 m, 3200 m, 6400 m, 12800 m and 25600 m. The I1 and I2 errors of the L1 spline for a given spacing. In half of the cases, the I error of the L1 spline is smaller than the I error of the corresponding L2 spline. In the other half of the cases, it is larger. Overall, this evidence indicates that L1 splines preserve shape better for this terrain data set than do L2 splines.

Lee, A., Snouffer, R., Easter, R., Foti, J., and Casar, T.	Security Requirements for Cryptographic Modules	FIPS 140-2 (http://csrc.nist.gov/publications)	7/10/2001
--	---	---	-----------

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic

Author	Title	Place of Publication	Date
Lennon, E.B., Simon, K.K., Helfer,	ITL Technical Accomplishments 2000	NISTIR 6558	10/31/2000

The ITL Technical Accomplishments 2000 report presents the achievements and highlights of NIST's Information Technology Laboratory (ITL) during FY 2000. Technical projects in eight divisions are described, followed by industry interactions, international activities, staff recognition, and service to the NIST staff and public.

Liggett, W. Query Expansion Seen Through Return Order of Relevant Documents Included in NIST SP 500-249 10/1/2001

There is a reservoir of knowledge in data from the TREC evaluations that analysis of precision and recall leaves untapped. This knowledge leads to better understanding of query expansion as this paper demonstrates. In many TREC tasks, the system response required is an ordered list of 1000 document identifiers. Instead of just using the identifiers to determine the positions of relevant documents in each list, we extract from each list the identifiers of the relevant documents and compare document ordering in these sub-lists. In other words, we consider the return order of relevant documents. We use Spearman's coefficient of rank correlation to compare sub-lists and multidimensional scaling to display the comparisons. Applying this methodology to data from the TREC Query Track, specifically, to system responses to twenty restatements of each of four topics, we show how two systems with query expansion differ from four systems without. We observe return-order variations caused by topic restatement and determine how query expansion affects these variations. For some topics, query expansion reduces the sizes

Liggett, W., Over, P. Understanding TREC Results - The Role of Statistics Proceedings of the 53rd Session of the International Statistical Institute

The challenge in empirical development of information retrieval systems at TREC is obtaining general conclusions from IR system responses to a sample of perhaps 50 topics, that is, 50 statements of information need. Treating such a sample as a simple random sample and using a univariate performance measure to describe each search result does not provide sufficient sensitivity for many purposes. In this paper, we contend that greater sensitivity can be gained through study of the natural language basis for the dependence of system performance on topic.

Lyon, G.E. Digital Rights, Risk and Assurance NIST Technical Note

A trust and assurance perspective applies readily to the distribution of digital products over the Internet: It identifies when digital rights remain viable, even with eventual mishaps and leaks that attend every long-term operation. An assurance system needs a flexible framework that is not too expensive. Arguments identify six preliminary assurance factors and briefly sample the rich space defined by them. The results illustrate that digital rights management can work in important cases, such as digital cinema. Other examples highlight circumstances that are not easily handled: Peer-to-peer distribution falls into this latter

Lyon, G.E. The Internet Marketplace and Digital Rights Management NISTIR 6765 and Paper 202 in Proceedings of SSGRR2001 Conference on Infrastructure for e-Business, e-Education and e-Science on the Internet, Aug.6-12, 2001, L'Aquila, Italy

Lacking physical control over Internet receiving environments, traditional information security methods cannot fully protect digital products. Insisting upon physical control severely restricts the Web market for digital objects and stymies e-commerce. Early digital rights management (DRM) reflects this dilemma, providing only limited scopes of application and suffering from poor usability. Three views—of customers, of losses, and of applications—help clarify considerations for a less restrictive next-generation DRM. Suggestions include expanding the roles of (i) biometrics to ease everyday use and tighten identity binding, and (ii) third parties to substantiate participant credentials and reputations.

Author	Title	Place of Publication	Date
Lyon, G.E.	Comparison of Two Scalability Tests	Information Processing Letters	
<p>When a computer system is expensive to use or is not often available, one may want to tune software for it via analytical models that run on more common, less costly machines. In contrast, if the host system is readily available, the attraction of analytical models is far less. One instead employs the actual system, testing and tuning its software empirically. Two examples of code scalability testing illustrate how these approaches differ in objectives and costs, and, how they complement</p>			
Lyon, G.E., Tang, H.C.	Assurance Hierarchies in B2C Electronic Commerce	NISTIR 6713	2/14/2001
<p>Electronic commerce (e-commerce) is defined as a broad, interdisciplinary field addressing the automation of business practices via open, globally spanning, Internet public access. E-commerce shows great promise in improving the efficiency of current business practices and in fostering completely new forms of business transactions. However, business concerns must be addressed in pursuing commercial objectives on the Internet. Assurance is among these: Identity, trust, and reputation are essential elements in any business deal. Unfortunately, with physical presence lacking, Internet business participants must rely upon other means to establish identity and assess reputation. The discussion explores frameworks for establishing assurance</p>			
Marbukh, V.	Network Management Under Incomplete Information on the Operational Environment	Proceedings of International Symposium on Information Theory & Applications (ISITA 2000), Honolulu, HI, 11/5-8/00	11/5/2000
<p>This paper proposes an approach to network management under incomplete information on the operational environment. The approach employs a combination of the minimax and Bayes' methodologies for making network management decisions under uncertainty. As an example we consider loss networks.</p>			
Martin, A.F., Przybocki, M.A.	Speaker Recognition in a Multi-Speaker Environment	7th European Conference on Speech Communications and Technology, Eurospeech 2001	
<p>We discuss the multi-speaker tasks of detection, tracking, and segmentation of speakers as included in recent NIST Speaker Recognition Evaluations. We consider how performance for the two-speaker detection task is related to that for the corresponding one-speaker task. We examine the effects of target speaker speech duration and the gender mix within test segments on results for these tasks. We also relate performance results for the tracking and segmentation tasks, and look at</p>			
Martin, A.F., Przybocki, M.A.	The NIST Speaker Recognition Evaluations: 1996-2001	2001: A Speaker Odyssey, A Speaker Recognition Workshop	
<p>We discuss the history and purpose of the NIST evaluations of speaker recognition performance. We cover the sites that have participated, the performance measures used, and the formats used to report results. We consider the extent to which there has</p>			

Computer-supported cooperative work (CSCW) aims to provide similar improvements for “multiple individuals working together in a conscious way in the same production process or in different but related production processes.” (Marx 1867) If achieved, this aim, which has proven elusive during the relatively few years since the term CSCW was coined in 1984, promises to multiply our productivity, perhaps by more than the square of the number of users, as compared against the productivity improvements that personal computers provide to each of us as individuals. In this article we consider the main challenges that impede us from realizing the great promise of CSCW, and then we discuss some of the key features that CSCW must provide in order to succeed with users. We follow this with a picture of the current state of the practice among CSCW users, and then we examine some technologies that hold promise for future application to CSCW. When considering these promising technologies, we suggest links between past CSCW research and related emerging, commercial technologies, and we also identify some current research that holds great potential for future application to CSCW. We close with some speculation on the future of CSCW. Before proceeding along these lines, however, we open by considering various definitions for CSCW, and related terms, and by drawing outlines around the large scope covered by CSCW. In this article, we specifically survey different ground than Mahling (2000) covered in his excellent article on CSCW included in the first edition of this encyclopedia. We refer interested readers to that article for additional, complementary insights on CSCW.

Mink, A., Salamon, W.J., Editors

Proceedings of the 2nd Annual Digital
TV Application Software Environment
(DASE)
Symposium 2001: End-to-End Data

NISTIR 6740

6/19/2001

This document contains presentation slides for the proceeding of the 2nd Annual Digital TV Application Software Environment (DASE) Symposium 2001: End-to-End Data Services, Interoperability & Applications. The conference is co-sponsored by NIST and ATSC and is to be held at NIST, Gaithersburg, MD, 19-20 June 2001.

Mitchell, W.F.

A Refinement-Tree Based Partitioning
Method for Adaptively Refined Grids

Accepted by Proceedings of the
Tenth SIAM Conference on Parallel
Processing for Scientific Computing

The partitioning of an adaptive grid for distribution over parallel processors is considered in the context of adaptive multilevel methods for solving partial differential equations. A k-way refinement-tree based partitioning method is presented. Numerical results comparing it with recursive coordinate bisection and a multilevel diffusive method from ParMETIS show that it runs and order of magnitude faster than the multilevel diffusive method and produces partitions of similar quality.

Mitchell, W.F.

Adaptive Grid Refinement and Multigrid
on Cluster Computers

Accepted by Proceedings of the
15th International Parallel and
Distributed Processing Symposium

It has been shown that the combination of adaptive grid refinement and multigrid solution, known as adaptive multilevel methods, provide effective methods for solving partial differential equations on sequential computers. Recently, research has been performed on parallelizing these procedures. Effective parallelization is difficult because of the irregular nature of both adaptively refined grids and the multigrid process. This is particularly true on cluster computers, which have slow communication channels that require algorithms with infrequent communication. An approach to parallelizing adaptive multilevel methods with few communication steps is presented. Numerical results on an 8-processorPC cluster demonstrate 60-90 percent efficiency.

Author	Title	Place of Publication	Date
Morse, E.L., Steves, M.P.	A Visualization Approach to Dealing with Log Data	Website of the Workshop on Data Log Mining of the Computer Supported Cooperative Work Conference	
<p>The CollabLogger is a visual tool that supports usability analyses of human-computer interaction in a team environment. Participants in our computer-mediated activity were engaged in a small-scale manufacturing testbed project. Interactions of the group were mediated by Teamwave Workplace and the members performed both synchronous and asynchronous activities depending on their availability, project requirements, and due to chance meetings in the collaborative space. The software was instrumented to log users' interactions with the system and each other. The CollabLogger addresses the problem of helping investigators analyze the volumes of log data that groupware tools can generate. Visual tools are powerful when large amounts of diverse data present themselves. The place-based collaboration environment offered by Teamwave Workplace provided a level of organization that allowed us to create a visual interface with which to perform exploratory sequential data analysis. Preliminary use of the tool shows that usability engineers can employ the visual display to form hypotheses about subject's</p>			
Nakassis, A., Youssef, A.	User Metrics for Digital Libraries	2001 International Conference on Imaging Science, Systems, and Technology (CISST'2001) Las Vegas, Nevada 6/25-28/2001	
<p>The libraries of the future will be, predominantly, digital with multimedia content. They will require new techniques for querying, indexing and retrieval, and responding to users. They will also require adapted and new performance measurement procedures. The paper addresses the problem of how to modify and supplement existing library metrics so as to be able to perform measurements. The paper also describes automated tools for benchmarking the performance of indexing algorithms.</p>			
Okun, V., Black, P.E., Yesha, Y.	Fault Classes and Fault Coupling in Boolean Specifications	ACM Transactions on Software Engineering Methodology	
<p>Fault-based testing strategies generate tests to detect faults belonging to a preselected set of simple fault classes. A hierarchy of fault classes and the infrequency of fault coupling let us rely on these strategies to detect many other faults, too. For Boolean specifications, Kuhn proved that there is a hierarchy of fault classes with respect to detectability. This implies that some fault classes may be ignored during test generation. We prove that Kuhn's hierarchy holds for a general form of Boolean specifications, then consider detectability of another fault class. Fault coupling occurs when a test set can detect faults in isolation, but not in combination; a low incidence of fault coupling is desirable. Using Kuhn's technique, we show that fault coupling does not occur for some important fault classes in expressions containing a restricted set of Boolean operators.</p>			
O'Leary, D.	Iteration Method for the Solution of the Eigenvalue Problem of Linear Differential and Integral Operators	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications	1/31/2001

of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 77-80

O'Leary, D.	Methods of Conjugate Gradients for Solving Linear Systems	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 81-85	1/31/2001
-------------	---	---	-----------

Author	Title	Place of Publication	Date
Patel, J.K., Kim, S.U., Su, D.H., Subramaniam, S., Choi, H.A.	A Framework for Managing Faults and Attacks in All-Optical Transport	Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX II), Anaheim, California, June 12-14, 2001	

Fault and attack survivability in all-optical transport networks (AOTNs) require new approaches because of unique transmission characteristics. Specifically, fiber non-linearities and network transparency to transmitted signal types may make the network vulnerable to unorthodox attacks. Furthermore, unlike in electronic networks that regenerate signals at every node, attack detection and isolation schemes may not have access to the overhead bits used to transport supervisory information between regenerators or switching sites to perform their functions. This paper presents a discussion on attack scenarios and proposes a conceptual framework for modeling faults and attacks in AOTNs.

Phillips, P.J., Newton, E.M.	Meta-Analysis of Face Recognition Algorithms	NISTIR 6719 and Proceedings of International Conference on Computer Vision
------------------------------	--	--

To obtain a quantitative assessment of the state of automatic face recognition, we performed a meta-analysis of performance results of face recognition algorithms in the literature. The analysis was conducted on 24 papers that report identification performance on frontal facial images and used either the FERET or ORL database in their experiments. The 24 papers contained 68 performance scores that included 40 performance scores on novel algorithms, and matching baseline performance scores for 33 of the 40 scores. There are three main conclusions from the analysis. The first conclusion is that the majority of experiments do not adequately model challenging problems and their results have saturated performance levels. The second

Author	Title	Place of Publication	Date
Prins, J.	NIST/SEMATECH Engineering Statistics Handbook Chapter 6: Process or Product Monitoring and Control	Web	
<p>This chapter presents techniques for monitoring and controlling processes and signaling when corrective actions are necessary. It covers both statistical process control (SPC) and statistical quality (SQC). SPC is based on a comparison of what is happening today with what happened previously to guarantee that process has not degraded. SQC is a technique for inspecting enough product from given lots to ensure a specified quality level.</p>			
Przybocki, M.A., Martin, A.F.	Odyssey Text Independent Evaluation Data	2001: A Speaker Odyssey, A Speaker Recognition Workshop	
<p>We discuss the text-independent data supplied for the 2001: A Speaker Odyssey evaluation track. We cover the data creation and selection process, and we present results restricted to the Odyssey test set for participating systems in the 2000 NIST Speaker Recognition Evaluation.</p>			
Reeker, L.H.	Theoretical Constructs and Measurement of Performance and Intelligence in Intelligent Systems	NIST SP 970	
<p>This paper makes a distinction between measurement at surface and deeper levels. At the deep levels, the items measured are theoretical constructs or their attributes in scientific theories. The contention of the paper is that measurement at deeper levels gives predictions of behavior at the surface level of artifacts, rather than just comparison between the performance of artifacts, and that this predictive power is needed to develop artificial intelligence. Many theoretical constructs will overlap those in cognitive science and others will overlap ones used in different areas of computer science. Examples of other "sciences of the artificial" are given, along with several examples of where measurable constructs for intelligent systems are needed and</p>			
Remington, K.A., Pozo, R.	NIST Sparse BLAS User's Guide	NISTIR 6744	5/9/2001
<p>This document provides a guide and reference manual for a portable numerical library for sparse matrix computations. These Basic Linear Algebra Subprograms (BLAS) provide kernels for forming sparse matrix products (of the form $C = aAB + bC$, where a and b are scalars, B and C are dense matrices, and A is a sparse matrix) and solution of triangular systems with left and right scaling ($C = aLATRB + bC$, where a and b are scalars, L and T are diagonal matrices, T is the conceptual inverse of a triangular sparse system, and B and C are dense matrices). Complete function listings for the ANSI C programming language are</p>			
Ressler, S.	A Web-Based 3D Glossary for Anthropometric Landmarks	HCI International 2001, New Orleans, LA, August 5-10, 2001	
<p>We have created a visual 3D anthropometric landmark glossary usable over the Web. Implemented using VRML, the Virtual Reality Modeling Language, users may easily locate and determine the names of these landmarks. Landmarks are visualized as</p>			

small spheres located over the body. Users can select the landmark name and the display is adjusted to place the viewer in front of that location. In addition users can select from among different landmark nomenclatures. The landmarks also highlight when selected, giving visual feedback. In addition a number of reference planes, such as the Frankfort plane and the coronal, sagittal and transverse planes can be turned on or off. Additional display controls are available via a movable control panel. The initial set of landmark names comes from the CAESAR (Civilian American and European Surface Anthropometry Resource) project. Three versions of the system have been implemented. The first is a head only model. Names for the head model are displayed simply by moving the cursor over the spheres and no selection is needed. The other two versions, requiring the user to click a selection, function identically and illustrate the landmarks for a standing male and for a male in a wheel chair.

Author	Title	Place of Publication	Date
Ressler, S., Antonishek, B., Wang, Q., Godil, A.	Integrating Active Tangible Devices with a Synthetic Environment for Collaborative Engineering	Web3D 2001 Symposium, Paderborn, Germany, February	2/19/2001

This paper describes the creation of an environment for collaborative engineering. in which the goal is to improve the user interface by using haptic manipulation with synthetic environments. We have integrated a multiuser synthetic environment with physical robotic devices to create a work environment. These devices can move under computer control or may be manipulated directly by the user. The work environment represents objects from the application domain such as a building construction environment or manufacturing cell. Collaborating engineers can discuss object interactions, such as crane planning or building placement using this environment. A physical representation of a work environment enables the user to perform direct, tangible manipulations of the devices which are mirrored in the synthetic environment. The direct physical manipulation of robotic devices offers the users a natural and efficient method of interacting with the synthetic environment.

Roberts, J.W., Kelley, E.F.	Measurements of Static Noise in Display Images	SPIE Electronic Imaging '01 Conference
-----------------------------	--	--

The appearance of noise on a display is an important usability issue. Sources of noise include electrical interference, display driver artifacts, resampling artifacts, transmission artifacts, compression artifacts, and any intrinsic noise artifacts produced within a display device. Issues for the severity of the noise problem include total magnitude of noise, noise spatial frequencies, proximity of the noise spatial frequencies to the spatial frequencies of the desired information content and the human-eye response to that information content, uniformity of the distribution of noise, and appearance of any visible or regular patterns in the noise. Whatever the source, inaccurate method to measure noise may be required to properly assess the influence of the

noise. We investigate the intricacies of using a digital camera to accurately measure noise in a static image on a flat panel display (FPD). The electro-optical transfer function of the FPD is measured. A known noise pattern is displayed and measured using the digital camera whereby the predicted noise is compared to the measured noise. Complications and limitations in the

Rosenthal, L.S., Brady, M.C.

What is This Thing Called

ITL Bulletin, January 2001, and XML
2000 Conference Proceedings,
December 2000

1/9/2001

XML developers claim they do it. OASIS, NIST, and W3C are building it. And, standards often require it. What is it? Conformance is usually defined as a way to determine if an implementation faithfully meets the requirements of a standard or specification. There are many types of testing including testing for performance, robustness, behavior, functions and interoperability. Although conformance testing may include some of these kinds of tests, it has one fundamental difference -- the requirements or criteria for conformance must be specified in the standard or specification. Conformance testing is meant to provide the software developers and users of conforming products some assurance or confidence that the product behaves as expected, performs functions in a known manner, or has an interface or format that is known. Determining whether a product faithfully implements the W3C Recommendations will be essential to creating robust, interoperable solutions. In this session, we will present an overview of conformance including what it is, how it works, and what are the benefits. Following the general conformance discussion will be specific examples from available conformance test suites including, XML, DOM, and XSLT. In addition, we will discuss particular problems that we have uncovered as a result of developing the tests, and give an indication of how various implementations fare against the available test suites.

Author	Title	Place of Publication	Date
Rossiter, W.J., Jr., Vangel, M.G., McKnight, M.E., Signor, A., Byrd,	Ultrasonic Extraction/Anodic Stripping Voltammetry for Determining Lead in Household Paint: A Laboratory	NISTIR 6571	

A laboratory study was conducted to evaluate the reliability of commercial, field-portable ultrasonic extraction-anodic stripping

voltammetry (UE/ASV) for determining the lead levels of laboratory-prepared paint films when tests were performed by certified lead inspectors trained to conduct UE/ASV testing. Two factory-calibrated UE/ASV apparatuses from the same supplier were purchased and used to conduct an experiment investigating the effects of lead level, apparatus, lead pigment type, operator, paint-film substrate, and overlayer applied to the lead-based paint film. Test panels, with either white lead (i.e., basic lead carbonate) or lead chromate pigments, had 10 lead levels

ranging from 0 mg/cm² to 3.5 mg/cm². The lead-based paint films were adhered to steel or plaster substrates, which were considered for experimental design purposes to be difficult or easy to sample, respectively. The overlayers were either a thickly applied oil-based paint (about 0.75 mm to 1.4 mm) or a thinly applied latex paint (about 0.13 mm to 0.28 mm). The five operators were trained by a UE/ASV supplier's representative to conduct the tests using a written protocol developed from the supplier's instructions. The study showed that one of the two ASV electrochemical instruments was in calibration, whereas the response of the second ASV instrument was low at the lower lead concentrations used to check calibration. Consequently, the data were analyzed both as "unadjusted for calibration" and "adjusted for calibration." Lead levels determined by the UE/ASV tests were often considerably less than the lead levels in the test panels. Depending on the combination of five experimental factors—apparatus, operator, lead pigment type, substrate type, and overlayer—the recovered lead for the data adjusted for calibration ranged from 28 % to 94 %, with the median recovery being 63 %. These findings are in sharp contrast with previously published results of an UE/ASV field study in which lead recoveries generally ranged from 75 % to more than 100 %. In the present study, ASV measurement error did not appear to play a role in the low lead recoveries based on quality assurance measures. A key contributor appeared to be incomplete lead solubilization during paint specimen sonication. The major experimental factor affecting UE/ASV response was overlayer, with test panels having thick-oil overlayers yielding lower lead recoveries than those with thin-latex overlayers. It may have been that thick-oil overlayers were more difficult to sonicate, and/or grind before sonication, than thin-latex overlayers. Effects of the other experimental factors on UE/ASV response were considered primarily for the calibration-adjusted data. Operator and substrate factors were found to have a significant effect;

Russakoff, D., Herman, M.

Head Tracking Using Stereo

International Journal of Machine
Vision and Applications

Head tracking is an important primitive for smart environments and perceptual user interfaces where the poses and movements of body parts need to be determined. Most previous solutions to this problem are based on intensity images and, as a result, suffer from a host of problems including sensitivity to background clutter and lighting variations. Our approach avoids these pitfalls by using stereo depth data together with a simple human torso model to create a head tracking system that is both fast and robust. We use stereo data to derive a depth model of the background which is then employed to provide accurate foreground segmentation. We then use directed local edge detectors on the foreground to find occluding edges which are used as features to fit to a torso model. Once we have the model parameters, the location and orientation of the head can be easily estimated. A useful side effect from using stereo data is the ability to track head movement through a room in three

Rust, B.W.

Fitting Nature's Basic Functions Part II.
Estimating Uncertainties and Testing
Hypotheses

Computing in Science and
Engineering 3, No. 6 (Nov/Dec

11/1/2001

This paper is the second in a series on fitting combinations of basic mathematical functions to measured data from the real world. This installment explains statistical diagnostic techniques for evaluating linear least squares fits. Topics covered include the variance and correlation matrices for the least squares estimate, construction of confidence intervals for the estimate, and

testing hypotheses about the statistical significance of the individual components of the estimate. The use of the techniques is illustrated by applying them to the analysis of polynomial fits to the measured global average annual temperature record for the

Author	Title	Place of Publication	Date
Rust, B.W.	Fitting Nature's Basic Functions I. Polynomials and Linear Least Squares	NIST Journal of Research and Computing in Science and Engineering 3, No. 5 (Sept/Oct 2001), pp. 84-89	10/1/2001

This paper is the first in a series on fitting combinations of basic mathematical functions to measured data from the real world. This installment explains linear least squares with a special emphasis on polynomial fits. It describes the statistical assumptions in the general linear model and explains why the least squares calculation gives the best linear unbiased estimate for the unknown parameters. It uses the measured global average annual temperature record for the years 1856-1999 as an example data set and compares the extrapolations into the future of various polynomial fits to that data set.

Scholtz, J.C.	Government Roles in HCI	Chapter in Handbook of Human-Computer Interaction to be published by Elsevier in 2002
---------------	-------------------------	---

The chapter describes the key roles that governments play in human-computer interaction: as users of software, producers of information, legislators of standards, and funders of research. For each of these sections the issues involved are described and case studies are briefly described and referenced for further investigation by the readers.

Scholtz, J.C., Laskowski, S.J., Morse, E.L., Wichansky, A., Butler,	Quantifying Usability: The Industry Usability Reporting Project	"Interacting With Computers" special edition based on submissions of the Conference on
---	---	--

Usability is an important concept for both the users of software and the producers of software. But, what exactly is usability? How can usability be measured or quantified? How much does usability testing save or cost? Can an environment be created that encourages incorporating usability engineering into the software development lifecycle? The Industry Usability Reporting (IUSR) Project seeks to help potential corporate consumers of software obtain information about the usability of supplier products, to measure the benefit of more usable software, and to increase communication about usability needs between consumers and suppliers. There are two parts to the IUSR Project: 1) a proposed format for sharing usability information and a pilot study in which both supplier (the developer) and consumer (the purchaser) companies to test the effectiveness of using

usability test results as procurement criteria, and 2) a pilot study to verify the usefulness of the reporting format. These are the first steps along a path to creating usability tools and techniques that can serve to increase communications across corporate

Sekerka, R.F., Coriell, S.R.,
McFadden, G.B.

Separation of Scales for Growth of an
Alloy Needle Crystal

Accepted by Metallurgical and
Materials Transactions

We reexamine the problem of a needle crystal (a model for a dendrite primary stalk) having the shape of a paraboloid of revolution growing at constant velocity from a supercooled binary alloy with given bulk concentration and far-field temperature. The coupled problem of thermal and solutal diffusion has been studied by a number of authors, including Ivantsov, Bolling & Tiller, Langer, and Lipton, Glicksman, & Kurz. We discuss the form of the analytical relation between the growth rate and the undercooling. For typical material properties in a metallic system, there is an obvious separation of scales of thermal and solutal effects, and this relation has the form of a doubly sigmoidal function, with a nearly flat intermediate region where the two sigmoids join. To the left of this nearly flat region, the dendrites are 'solutal' with negligible contributions from the thermal field, whereas to the right of this region, they are 'thermal' with the solutal contribution fixed at its value for unit supersaturation.

Author	Title	Place of Publication	Date
Simon, M.J., Bentz, D.P., Filliben,	Concrete Optimization Software Tool User's Guide	Federal Highway Administration Internal Report	
<p>This user's guide provides instructions for and examples of using the Concrete Optimization Software Tool (COST), a joint product of the Federal Highway Administration and the National Institute of Standards and Technology. COST provides an internet-based system for optimizing concrete performance based on statistical experiment design and analysis methods. Working with local raw materials, COST designs an experimental program of concrete mixtures to be prepared and evaluated. In these mixtures, the user can vary the water-to-cement (w/c) ratio and other concrete mixture parameters such as the cement, mineral and chemical admixture, and aggregate contents. Once the measured responses (properties) for the prepared concretes are input into the COST system, it analyzes the results and determines the optimum mixture proportions based on user-supplied performance criteria. Results and analysis are provided in both graphical and numerical formats to aid in interpretation. Typical uses of COST might be to design a concrete that meets all specifications at minimum cost or to design a concrete that</p>			

Sims, J.S., Hagedorn, J.G.,
Ketcham, P.M., Satterfield, S.G.,
Griffin, T.J., Am Ende, B.A., Hung,
H.K., Martys, N.S., Bouldin, C.P.,
Warren, J.A., Feder, D.L., Clark,
C.W., Fowler, H.A., Filla, B.J.,

Accelerating Scientific Discovery
Through Computation and Visualization

NISTIR 6709 and NIST Journal of
Research, Vol. 105, No. 6,
November-December 2000

1/1/2001

Scientific discovery can be accelerated through computation and visualization. This acceleration results from the synergy of expertise, computing tools and hardware for enabling high-performance computation, information science and visualization that is provided by a team of computation and visualization scientists collaborating in a peer-to-peer effort with the research scientists. In the context of this discussion, {em high performance} refers to capability beyond the current state of the art in desktop computing. To be effective in this arena, a team comprising a critical mass of talent, parallel computing techniques, visualization algorithms, advanced visualization hardware and a recurring investment is required to stay beyond the desktop capabilities. This article describes, through examples, how the Scientific Applications and Visualization Group (SAVG) at NIST has utilized high performance parallel computing and visualization to accelerate scientific discovery. The examples include scientific collaborations that have advanced research in the following areas: (1) Bose-Einstein Condensate Modeling, (2) Fluid Flow in Porous Materials and in Other Complex Geometries, (3) Flows in Suspensions, (4) X-ray Absorption, (5) Dielectric

Snouffer, S.R., Lee, A.

A Comparison of the Security
Requirements for Cryptographic
Modules in FIPS 140-1 and FIPS 140-2

ITL Bulletin, July 2001

7/9/2001

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. A documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1&2 and other cryptographic standards is specified in the Derived Test Requirements. FIPS 140-1 is one of NIST's most successful standards and forms the very foundation of the Cryptographic Module Validation Program. FIPS 140-2 addresses lessons learned from questions and comments and reflects changes in technology. The standard was strengthened, but not changed in focus or emphasis. Also, the standard was minimally restructured to:- Standardize the language and terminology to add clarity and consistency, -Remove redundant and extraneous information to make the standard more concise, and - Revise or remove vague requirements. Finally, a new section was added detailing new types of attacks on cryptographic modules that currently do not have specific testing available. The differences paper summarizes the changes from FIPS 140-1 to FIPS 140-2 and documents the detailed requirements. This bulletin summarizes the differences paper.

Author	Title	Place of Publication	Date
Snouffer, S.R., Lee, A., Oldehoeft, A.E.	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2	NIST SP 800-29 (http://csrc.nist.gov/publications)	6/1/2001

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. A documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1&2 and other cryptographic standards is specified in the Derived Test Requirements. FIPS 140-1 is one of NIST's most successful standards and forms the very foundation of the Cryptographic Module Validation Program. FIPS 140-2 addresses lessons learned from questions and comments and reflects changes in technology. The standard was strengthened, but not changed in focus or emphasis. Also, the standard was minimally restructured to:- Standardize the language and terminology to add clarity and consistency, -Remove redundant and extraneous information to make the standard more concise, and - Revise or remove vague requirements. Finally, a new section was added detailing new types of attacks on cryptographic modules that currently do not have specific testing available. This differences paper summarizes the changes from FIPS 140-1 to FIPS 140-2 and documents the detailed requirements.

Sterling, D.G.	Chaotic Synchronization of Ergodic	Accepted by Chaos
----------------	------------------------------------	-------------------

Self-synchronizing chaotic systems can be used as synchronous pseudo-random sequence generators, though physical applications have been limited by the sensitivity of the synchronous state to noise. Using two separate time scales in conjunction with a digital filter suppresses the noise in the coupling signal. We find this gives stable synchronous motion even for signal-to-noise ratios less than 1. As an application of these pseudo-random sequence generators we propose a chaotic modulation scheme based on ergodic maps. We characterize the performance of this system by bounding the mean

Stoneburner, G.R.	Security - Revenue Generator and Mission Enabler	Proceedings of the 2001 Annual Computer Security Applications Conference, New Orleans, Louisiana, Dec. 10-14, 2001
-------------------	--	--

We need to facilitate a change in user perception of security from a hindrance to an essential revenue generator and mission enabler. The Common Criteria protection profile (PP) and security target (ST) constructs can be used to help achieve this need. Yet this will only be possible if current, common PP/ST development practices are changed.

Stoneburner, G.R.	Underlying Technical Models for Information Technology Security	NIST SP 800-33
-------------------	---	----------------

Underlying Technical Models for Information Technology Security provides a description of the technical foundations, termed 'models', that underlie secure information technology (IT). The intent is to provide, in a concise form, the models that should be considered in the design and development of technical security capabilities. These models encompass lessons learned, good

practices, and specific technical considerations. The intended audience consists of both government and private sectors including IT users desiring a better understanding of system security, engineers and architects designing/building security capabilities, and those developing guidance for others to use in implementing security capabilities.

Stoneburner, G.R.	Engineering Principles for Information Technology Security	ITL Bulletin, June 2001	6/19/2001
-------------------	---	-------------------------	-----------

In June 2001, ITL released NIST Special Publication (SP) 800-27, Engineering Principles for Information Technology Security (EP-ITS), by Gary Stoneburner, Clark Hayden, and Alexis Feringa. Engineering Principles for Information Technology (IT) Security (EP-ITS) provides a list of system-level security principles to be considered in the design, development, and operation of an information system. This bulletin presents an overview of the document.

Author	Title	Place of Publication	Date
Stoneburner, G.R., Hayden, C., Feringa, A.	Engineering Principles for Information Technology Security	NIST SP 800-27 (http://csrc.nist.gov/publications)	6/1/2001

The Engineering Principles for Information Technology (IT) Security (EP-ITS) presents a list of system-level security principles to be considered in the design, development, and operation of an information system. This document is to be used by IT security stakeholders and the principles introduced can be applied to general support systems and major applications. EP-ITS presents principles that apply to all systems, not ones tied to specific technology areas. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. While the primary focus of these principles remains on the implementation of technical countermeasures, these principles highlight the fact that, to be effective, a system security design should also consider

Stutzman, P.E., Leigh, S.	Compositional Analysis of NIST Reference Material Clinker 8486	Accuracy in Powder Diffraction Conference, NIST, April 2001	3/20/2001
---------------------------	---	--	-----------

Certification of the phase compositions of the NIST Reference Clinkers often is based upon more than one independent method. The current certificate values were established using an optical microscope examination and additional microscope data taken from an ASTM C 1356 round robin. The X-ray powder diffraction (XRD) study provides the second, independent estimate of the phase abundances, with the experiment designed to evaluate inter- and intra-vial homogeneity. Reitveld analysis of the powder diffraction patterns allowed calculation of a set of best-fit reference patterns and their scale factors. Because of significant contrast in the linear absorption coefficients of ferrite and periclase relative to the estimated mean matrix linear absorption coefficient, the scale factors were adjusted for microabsorption effects using the and the adjusted scale factors used to calculate phase abundance. The XRD data agree with the optical data with the exception of aluminates. This disagreement may

reflect the difficulty in resolving this finely-crystalline phase using the optical microscope. The XRD data did show greater precision than replicate measurements by microscopy.

Measurements from different sources, laboratories, instruments, and from different methods can exhibit significant between-method variability, as well as distinct within-method variances. The two data sets are treated using three methods to establish the best-consensus values and to provide meaningful uncertainties. While the mean values of the individual phase abundances do not vary, the 95 % uncertainty level values do. One method of combining the data sets was favored as this method produces a weighted mean whose weighting scheme does not necessarily skew the consensus value in the direction of

Swanson, M.	Security Self-Assessment Guide for Information Technology Systems	NIST SP 800-26 (http://csrc.nist.gov/publications)	11/1/2001
-------------	---	---	-----------

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found

Swanson, M., Lennon, E.B. (editor)	Security Self-Assessment Guide for Information Technology Systems	ITL Bulletin, September 2001	9/12/2001
------------------------------------	---	------------------------------	-----------

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found

Author	Title	Place of Publication	Date
Tang, X., Zheng, J.	Reflectance Calibration Standard for Optical Discs	Proceedings of Optical Data Storage Topical Meeting 2001, Santa Fe, New Mexico, April 22-25,	4/22/2001

An accurate method for the determination of reflectance of reference discs has been developed at NIST. The discs can be

used as a traceable industry standard in the calibration of optical disc testing equipment.

Tang, X., Zheng, J.	High Precision Measurement of Reflectance for Films Under	NISTIR 6794 and Optical	
<p>An accurate method for the determination of reflectance for metal films under transparent substrates has been developed at the National Institute of Standards and Technology (NIST). In the measurement, only the first reflected beam from the film is useful for the calculation. An optical loss at both surfaces of the substrate has been taken into account. A refractive index of the substrate is also accurately measured and used to calculate the film reflectance for comparison. Our measurement accuracy is as high as 0.3%. These accurately measured films serve as a traceable industry standard of reflectance in calibration of optical disc testing equipment and in the manufacturing of secondary calibration discs.</p>			
Toth, P.R.	Understanding the Common Criteria Evaluation and Validation Scheme	ITL Bulletin, October 2000	10/5/2000
<p>This ITL Bulletin describes the Common Criteria Evaluation and Validation Scheme.</p>			
Van Dyck, R.E.	Classified Zerotree Wavelet Image Coding and Adaptive Packetization for Low Bit Rate Transport	IEEE Transactions on Circuits and Systems for Video Technology	
<p>In this paper, we suggest a novel robust image coding and adaptive packetization algorithm suitable for very low bit rate transport. This algorithm can be applied to any zerotree-based encoder such as the embedded zerotree wavelet coder of Shapiro and set partitioning in hierarchical trees by Said and Pearlman. We propose a very explicit segmentation and packetization method of an image bit stream, where the lowest frequency subband is separately encoded from the higher frequency subbands for unequal protection over a noisy channel. The trees in the higher frequency subbands are split, classified, and assembled for efficient image coding and packetization according to their initial threshold and subband. The use of these classified trees enables one to make robust packets, while giving priority to some packets. Each packet has a different initial threshold and can be decoded independently. In spite of relatively heavy overhead for packetization, our algorithm is comparable to the original zerotree-based image coders used in ours at low bit rates. Additionally, simulation results show that the new method is resilient</p>			
Van Dyck, R.E., Miller, L.E.	Distributed Sensor Processing Over an Ad Hoc Wireless Network: Simulation Framework and Performance Criteria	MILCOM 2001, McLean, Virginia, October 28-31, 2001	10/28/2001
<p>The evaluation of existing and future distributed sensor processing system concepts can be done well using simulation, provided that the simulation is faithful in representing both the medium in which the sensors interface with the phenomena that they measure or detect and the medium in which the sensors interface with each other to achieve a distributed mode of operation. In this paper, performance criteria for distributed sensor processing over ad hoc wireless networks are stated and an architecture for analysis and simulation of this kind of system is described.</p>			
Van Vaerenbergh, S., Coriell, S.R., McFadden, G.B.	Morphological Stability of a Binary Alloy: Temperature-Dependent	NISTIR 6586 and Journal of Crystal Growth	11/17/2001

The effect of the temperature dependence of the diffusion coefficient on the morphological stability of a binary alloy during directional solidification is treated by a linear stability analysis. The Soret effect is also included in the analysis. Specific calculations are carried out for a tin alloy containing silver for which the diffusion coefficient has a linear dependence on temperature. Although the temperature dependence of the diffusion coefficient has little effect on the critical concentration for the onset of morphological stability, it causes a significant effect on the wavelength at the onset of instability.

Author	Title	Place of Publication	Date
Voorhees, E.M.	Overview of the TREC-9 Question Answering Track	Included in NIST SP 500-249	10/1/2001

The TREC question answering track is an effort to bring the benefits of large-scale evaluation to bear on the question answering problem. The track has run twice so far, where the goal both times was to retrieve small snippets of text that contain the actual answer to a question rather than the document lists traditionally returned by text retrieval systems. The best performing system in TREC-9, the Falcon system from Southern Methodist University, was able to answer about 65% of the questions (compared to approximately 42% of the questions for the next best systems) by combining abductive reasoning with various natural language processing techniques. The 65% score is slightly less than the best scores for TREC-8 in absolute terms, but it represents a very significant improvement in question answering systems. The TREC-9 task was considerably harder than the TREC-8 task because the TREC-9 track used actual users' questions rather than questions constructed specifically for the

Voorhees, E.M.	Evaluation by Highly Relevant	Proceedings of the 24th Annual International ACM SIGIR Conference on Research and Development in Information
----------------	-------------------------------	--

Given the size of the web, the search engine industry has argued that engines should be evaluated by their ability to retrieve highly relevant pages rather than all possible relevant pages. To explore the role highly relevant documents play in retrieval system evaluation, assessors for the TREC-9 web track used a three-point relevance scale and also selected best pages for each topic. The relative effectiveness of runs evaluated by different relevant document sets differed, confirming the hypothesis that different retrieval techniques work better for retrieving highly relevant documents. Yet evaluating by highly relevant documents can be unstable since there are relatively few highly relevant documents. TREC assessors frequently disagreed in their selection of the best page, and subsequent evaluation by best page across different assessors varied widely. The discounted cumulative gain measure introduced by Jarvelin and Kekalainen increases evaluation stability by incorporating all

Voorhees, E.M.	The TREC Question Answering Track	Journal of Natural Language Engineering
----------------	-----------------------------------	---

The Text REtrieval Conference (TREC) question answering track is an effort to bring the benefits of large-scale evaluation to bear on a question answering (QA) task. The track has run twice so far, first in TREC-8 and again in TREC-9. In each case the

the contact micrometer. Based on this model, the probability distribution of the diameters is derived and two diameter estimates are presented. We illustrate and compare the diameter estimates using simulated data.

Watson, C.I.	NIST Special Database 29, Plain and Rolled Images from Paired Fingerprint Cards	NISTIR 6801	11/1/2001
--------------	---	-------------	-----------

This new NIST fingerprint database offers the user complete paired fingerprint cards that include all ten rolled fingerprints and the plain/flat impressions at the bottom of the card. Paired fingerprint cards are two sets of fingerprints for one individual captured at different dates. By including all the fingerprint data for the card pairs, a user can compare any combination of "plain" and "rolled" images. This database has 216 paired fingerprint cards. Each card is scanned at 19.7 ppm (500 ppi) and segmented into individual fingerprint images. The segmented images are compressed using WSQ compression at a compression ratio of 15:1 and stored in the ANSI/NIST data format[6]. Reference information is included in comment fields to help reconstruct the fingerprint card image if desired as well as a human defined classification for each fingerprint image.

Watson, C.I.	NIST Special Database 30, Dual Resolution Images from Paired Fingerprint Cards	NISTIR 6800	11/1/2001
--------------	--	-------------	-----------

This new NIST fingerprint database offers the user complete paired fingerprint cards that include all ten rolled fingerprints and the plain impressions at the bottom of the card scanned at both 19.7 ppm (500 ppi) and 39.4 ppm (1000 ppi). Paired fingerprint cards are two sets of fingerprints for one individual captured at different dates. This database allows a user to compare algorithm results on two resolutions of the same image and specifically for adjusting the WSQ compression algorithm to work with 39.4 ppm images. This database has 33 paired fingerprint cards scanned at both resolutions and segmented into individual fingerprint images. The fingerprint cards scanned at 19.7 ppm are stored on the first CDROM and the 39.4 ppm scanned cards are stored on the other three CDROMs (11 cards per CDROM). The segmented images are compressed using lossless JPEG (JPEG-L) compression and stored in the ANSI/NIST data format[6]. Reference information is included in comment fields to help reconstruct the fingerprint card image if desired as well as a human defined classification for each fingerprint

Widmann, J.F., Presser, C., Leigh,	Dynamic Range Limitations in Phase Doppler Interferometry Measurements	Atomization and Sprays
------------------------------------	--	------------------------

It has been well established that the dynamic range of phase Doppler interferometry (PDI) size measurements is limited by the photomultiplier tubes (PMT). A statistical method is presented to overcome this limitation by combining data sets collected over different size ranges (PMT gains). The method is discussed and validated using a simulation in which droplets are sampled from monomodal and multimodal size distributions. The technique is also applied to experimental data collected in a reacting methanol spray. Experimental measurements of monodisperse droplets and polydisperse particles are presented showing that PMT saturation does not preclude accurate size measurements when using modern frequency domain signal processors that operate with one-bit analog-to-digital conversion. The results presented question the accepted dynamic range limitation of PDI systems, as well as the methods of optimizing the PMT gain reported in the literature.

Author	Title	Place of Publication	Date
Williams, D., Alpert, B.	Causality and Waveguide Circuit	IEEE Transactions on Microwave Theory and Techniques 49, no. 4 (2001), pp. 613-623	
	We develop a new causal power-normalized waveguide equivalent-circuit theory that, unlike its predecessors, results in network parameters usable in both the frequency and time domains in a broad class of waveguides. Enforcing simultaneity of the voltages, currents, and fields and a power normalization fixes all of the parameters of the new theory with a single-normalization factor, including both the magnitude and phase of the characteristic impedance of the waveguide.		
Witzgall, C.J.	Paths, Trees, and Flowers	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 140-144	1/31/2001
Witzgall, C.J., Cheok, G.S.	Registering 3D Point Clouds: An Experimental Evaluation	NISTIR 6743	1/31/2001
	Four separate laser scans of a wooden box, taken from different vantage points, were examined in a laboratory setting. Visual and numerical registration methods, aimed at aligning the individual scan data with respect to a common frame, were explored. The numerical registration method aligns point clouds with triangulated elevated surfaces (TIN) optimizing residual-based measures-of-fit, as outlined in this report. Essential procedures for data filtering are described including methods for shadow delineation. Data phenomena beyond common noise were uncovered, particularly, "phantom points" resulting from split signals. Such points interfere with determining occlusions. Results from four experiments applying numerical and visual procedures are		
Yuan, J., Mills, K., Montgomery, D.	Exploring Collective Dynamics of Large-Scale Networks	NIST Journal of Research	
	A large-scale network, such as the Internet, comprises a complex system from which may emerge collective phenomena. Network researchers usually investigate cause and effect relationships in specific communication protocols, ignoring potentially significant effects from emergent behaviors. In our work, we specifically seek to identify and understand the collective behavior of large-scale networks. We propose a two-dimensional cellular-automata model to investigate collective behavior in a large-scale network from abstract mathematical representations of individual nodes. We suspect such models can promote better understanding of the spatial-temporal evolution of network congestion, and other emergent phenomena of large-scale networks. To search the behavior space of the model, we study dynamic patterns arising from complex interactions among traffic flows routed across shared network nodes, as we employ various configurations of parameters and two different congestion-control algorithms. In this paper, we focus on the relationship between network size and time scale. Specifically, we		

investigate the long-range dependence of aggregate arrival traffic and the number of congested nodes in the model at different system sizes and time granularities. We find that for a given network size long-range dependence decays as time granularity increases, but as network size increases long-range dependence exists at larger time granularity. This suggests that network size and time scale are two closely related facets in the global emergence of collective behavior in a large-scale network. We also find that the collective properties of sub-areas within a larger network differ from the collective properties for the same sub-areas when they are extracted from the larger network.

Zhang, N.F.

Statistical Process Monitoring for
Autocorrelated Data

Journal of Applied Mathematics and
Decision Sciences

In the past years statistical process methodologies have been widely used in industry for process monitoring. However, the assumption that the process data are statistically independent is often invalid. This article discusses the approaches to deal with process autocorrelation in regarding of using process control charts and process capability indices.