FY 2002 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
Alemyehu, N.	Analysis of Performance Variation Using Query Expansion	Journal of the American Society for Information Science and	

Information retrieval performance evaluation is commonly made based on the classical recall and precision based figures or graphs. However, important information indicating causes for variation may remain hidden under the average recall and precision figures. Identifying significant causes for variation can help researchers and developers to focus onopportunities for improvement which underlay the averages. This paper presents a case study showing the potential of a statistical repeated measures analysis of variance for testing the significance of factors in retrieval performance variation. The TREC-9 Query Track performance data is used as a case study and the factors studied are retrieval method,topic and their interaction. The results show that retrieval method, topic and their interaction are all significant. A topic level analysis is also made in order to see the nature of variation in the performance of retrieval methods across topics. The observed retrieval performances of expansion runs are truly significant improvements for most of the topics. Analyses of the effect of query expansion on

Allen, R.A., Cresswell, M.W., Guthrie, W.F., Linholm, L.W., Bogardus, H., Martinez de Pinillos, J.V., am Ende, B.A., Murabito, C.E., Bennett, M.H. J.V., am Ende, B.A., Murabito,	CD Reference Materials for Sub-Tenth Micrometer Applications	International Society for Optical Engineering (SPIE) Microlithology Symposium, March 3-8, 2002	3/3/2002

Prototype linewidth reference materials with Critical Dimensions (CDs) as narrow as 70 nm have been patterned in (110) silicon-on-insulator films. The sidewalls of the reference features are parallel, normal to the substrate surface, and have almost atomically smooth (lll) surfaces. Linewidth calibration begins with the measurement of the electrical CDs of multiple reference features located at a selection of die sites on a wafer. The absolute widths of the cross sections of a sub-set of reference features on several chips that are diced from the wafer are then subjected to High Resolution Transmission Electron Microscopy (HRTEM) imaging to determine their physical CDs by lattice-plane counting. Sample preparation for lattice-plane counting by HRTEM is destructive, and other reference features on the same chip become unusable for reference-material purposes. However, a calibration curve for converting the measured electrical CDs of reference features on other chips on the wafer, known as "product reference features," to their physical values is obtained. The uncertainty attributed to the physical CD values of the product reference features generally varies inversely with the linear correlation between the cross-section lattice-plane counts and the corresponding electrical CD measurements of the sub-set of reference features that were selected for HRTEM imaging. A linear correlation value of approximately 0.97 has been obtained from a sub-set of I2 HRTEM measurements. Ln this case, the uncertainty attributed to the physical CD values of the product reference features was typically 13 nm. An apparent time-dependence of the electrical CD of the as-patterned reference features is believed to be responsible for most of the product reference feature uncertainty. However, it has now been found that a forming-gas annealing treatment appears to prevent the reference time dependence and thus has the potential for reducing the uncertainty level.

Alpert, B.K., Chen, Y.	A Representation of Acoustic Waves in Unbounded Domains	NISTIR 6623	10/1/2002

Compact, time-harmonic, acoustic sources produce waves that decay too slowly to be square-integrable on a line away from the sources. We introduce an inner product, arising directly from Green's second theorem, to form a Hilbert space of these waves, and present examples of its computation.

am Ende, B.A., Cresswell, M.W., Allen, R.A., Headley, T.J., Guthrie, W.F., Linholm, L.W., Bogardus, E.H., Murabito, C.E.	Measurement of the Linewidth of Electrical Test-Structure Reference Features by Automated Phase-Contrast Image Analysis	Proceedings of the IEEE International Conference on Microelectronic Test Structures,	4/8/2002

NIST, Sandia National Laboratories, and International SEMATECH are developing a new type of linewidth standard for calibrating Critical Dimension (CD) metrology instruments for lithographic process control. The standard reference feature is the bridge of an electrical linewidth test structure that is patterned in a mono-crystalline silicon film. Phase-contrast images of the cross sections of a sample of the bridge features on each wafer, produced by High-Resolution Transmission-Electron Microscopy (HRTEM), are used to trace the measured electrical linewidths of the standard reference feature to the lattice constant of silicon. This paper describes the automated analysis of the phase-contrast images that was developed in order to minimize the cost

Anderson, D.M., McFadden, G.B., Wheeler, A.A.
A Phase-Field Model of Convection with Solidification
Proceedings of the 40th AIAA Aerospace Sciences Meeting, Reno, Nevada, January 14-17, 2002
1/14/2002

A phase-field model for the solidification of a pure material that incorporates convection has recently been developed. This model is a two-fluid model in which the solid phase is modeled as a sufficiently viscous fluid. The model allows for the solid and liquid phases to have different densities and hence allows for expansion or contraction flows upon solidification. In this paper we investigate numerically a simplified version of this model by considering solidification occurring between the two closely-spaced parallel plates of a Hele-Shaw cell. We assess two key aspects of the model: (1) the effect of density differences between the solid and liquid phases during dendritic growth and (2) the role played by the viscosity ratio between the solid and liquid phases.

Andreason, A., Beichl, I.
Estimating the Work in Integer
IEEE Computing in Science and Engineering

For a given set of numbers, the integer partitioning problem is to divide the numbers into two groups, so that the sums of the numbers in each group differ by the smallest amount possible. In a balanced perfect partition, the sums differ by only zero or one, and the numbers of elements in each group differ by only zero or one. This problem is known to be NP-complete [3], and as a result, heuristics have been developed that provide minimized partition[6] and cardinality[7] differences over time. It is not clear, however, how long these heuristics need to be run to find an acceptable answer. We have developed a method to estimate the amount of work required to fine an optimal solution to the problem. We have also developed a method to estimate how many balanced perfect partitions exist. We use a variation of a technique developed by Knuth for estimating the size of

Aviles, A.I.
Robustness Experiments with Two Variance Components
American Statistical Association 2001 Proceedings of the Section on Physical and Engineering Sciences

In many experimental settings, different types of factors affect the measured response. The factors that can be set independently of each other are called crossed factors. Nested factors cannot be set independently because the level of one factor takes on a different meaning when other factors are changed. Random nested factors arise from quantity designations and from sampling and measurement procedures. The variances of the random effects associated with nested factors are called variance components. Factor effects on the average are called location effects. Dispersion effects are the effects of the crossed factors on the variance of a response. For situations where crossed factors have effects on the different variance components, then sets of dispersion effects must be identified and estimated to achieve robustness. The main objective of this research is to provide nearly D-optimal experimental design procedures for estimating the location effects of crossed factors, the variance components associated with two nested factors, and the dispersion effects that crossed factors may have on the two variance components. A general class of experimental designs for mixed-effects models with random nested factors, called assembled designs, is introduced in Avilés (2001). The use of assembled designs for robustness experiments is presented. In this paper, a practitioner's guide is presented for the use of assembled designs to estimate the location effects, the dispersion effects, and two variance components. A heuristic algorithm for finding a nearly D-optimal assembled design with two variance components for a given budget is provided. Ready to use computer programs for the presented experimental design procedures and analysis technique are also available. This paper is a "HOW TO" manual for robust design for the case

Ban, K., Gharavi, H.	IEEE 802.11 FHSS Receiver Design for Multihop Sensor Application	Conference Proceedings: 2002 International Conference on Broadband Wireless Access Systems, San Francisco, May 31,	5/31/2002

This paper presents a receiver design for IEEE 802.11 FHSS (Frequency-Hopping Spread-Spectrum) wireless local area network systems. 802.11 FHSS systems support two basic data rates. 1 Mbps and 2 Mbps systems employ 2GFSK (Gaussian Frequency Shift Keying) and 4GFSK modulation, respectively. Noncoherent receivers are generally preferred for the 802.11 FHSS system. This is due to their practical advantages over coherent receivers such as implementation cost and inherent robustness against frequency and carrier phase offset. In this paper we first discuss popular receiver design techniques such as the limiter-discriminator integrator detector (LDD) and differential detector (DD). These techniques are normally considered for GMSK (Gaussian Minimum Shift Keying) receivers. Since GFSK modulations suffer from inter-symbol interference (ISI), even in the absence of channel distortions, designing a simple and yet efficient equalizer is expected to improve the receiver performance considerably. Thus, we have designed equalizers that are based on the Viterbi Algorithm (VA). We will show that such equalizers are very effective in improving the receiver performance, particularly in the case of 4GFSK modulation which is

Ban, K., Gharavi, H.	Video Transmission for Multi-Hop Networks Using IEEE 802.11 FHSS	Conference Proceedings: IEEE 2002 International Conference on Image Processing, New York, September 22-25, 2002	5/22/2002

In many applications such as construction, manufacturing, ground robotic vehicles, and rescue operations, there are many issues that necessitate the capability of transmitting digital video and that such transmissions should be performed wirelessly and in an ad-hoc manner. Recently, we proposed an ad-hoc, cluster-based, multihop network architecture for video communications. For implementation, the IEEE 802.11 FHSS wireless LAN system using 2GFSK modulation has been deployed. To enhance the overall throughput rate for higher quality video communications, we present a performance evaluation of the

IEEE 802.11 FHSS when 4GFSK modulation option is selected. Unfortunately, the 2 Mb/s system utilizing 4GFSK modulation is not very efficient in terms of RF range. Therefore, to improve its performance for multihop applications, a combination of diversity and non-coherent Viterbi based receiver is considered. For the video transmission part, we have considered a bitstream splitting technique together with a packet-based error protection strategy to combat packet drops under multipath fading conditions. Finally, the paper presents the simulation results, including the effects of the receiver design and diversity on the

Barker, E.B.	Cryptographic Standards and Guidance: A Status Report	ITL Bulletin, September 2002	9/20/2002

A comprehensive toolkit of cryptographic standards and associated guideline that covers a wide range of cryptographic technology is currently under development by the Computer Security Division at NIST. These standards and guidelines will enable U.S. Government agencies to select cryptographic security components and functionality for protecting their data communications and operations. This bulletin provides a status report on the development of these standards and guidelines and advises Federal agencies on their use. Advice provided in this bulletin includes 1) a warning that the use of single DES (as specified in FIPS 46-3) will no longer be approved when FIPS 46-3 comes up for review in 2004, 2) a recommendation that three distinct keys should be used when Triple DES is used for encryption (Triple DES was adopted in FIPS 46-3 and specified in ANSI X9.52), 3) a statement that all three AES key sizes are considered adequate for Federal Government applications (AES is specified in FIPS 197), and 4) a comparison of the use of AES and Triple DES. Web links to the current standards and guidelines

Beichl, I., Bernstein, J., Karim, A.	Automated Image Processing Tools for High Throughput Measurements of Polymer Coatings: Initial Report on Software to Quantify Features	NISTIR 6869	

We have developed a series of Matlab programs to analyze photographs of polymer dewetting. This report provides details of how the programs work, what they do, and how users canfine tune the output.Meredith, Smith, Karim and Amis have developed a method to gather massive amounts of data on the dewetting process for polymers, by using a combinatorial approach to data collection. These data, produced by automated microscopy, are collected in the form of photographs of polymers varying the parameters of temperature, thickness and time. The purpose of the tools described in this report is to identify features of the dewetting process and to quantify the features without having a human doing the feature recognition or the counting. The volume of the data makes human processing utterly impractical. In this report we describe methods used on photographs of three stages of dewetting. This report is preliminary. A setof tools to automate the analysis of the photographic images completely,

Beichl, I., Sullivan, F.	It's Bound to be Right	IEEE Computing in Science and Engineering 4 No.2 (2002), pp.86-90	

This is a tutorial article on a Monte Carlo method for eliminating double counting in massive data sets. It has also been used to classify images.

Bentz, D.P., Mizell, S., Satterfield, S., Devaney, J., George, W., Ketcham, P., Graham, J., Porterfield, J., Quenard, D., Vallee, F., Sallee, H., Boller, E., Baruchel,	The Visible Cement Data Set	NIST Journal of Research, Vol. 107, No. 2, March-April 2002,	4/1/2002

With advances in X-ray microtomography, it is now possible to obtain three-dimensional representations of a material's microstructure with a spatial resolution of better than one micrometer per voxel. The Visible Cement Data Set represents a collection of 3-D data sets obtained using the European Synchrotron Radiation Facility in Grenoble, France in September of 2000. Most of the images obtained are for hydrating portland cements pastes, with a few data sets representing hydrating Plaster of Paris and a common building brick. All of these data sets are being made available on the Visible Cement Data Set website at http://visiblecement.nist.gov. The website includes the raw 3-D datafiles, a description of the material imaged for each data set, example two-dimensional images and visualizations for each data set, and a collection of C language computer programs that will be of use in processing and analyzing the 3-D microstructural images. This paper provides the details of the experiments performed at the ESRF, the analysis procedures utilized in obtaining the data set files, and a few representative

Black, P.E., Ammann, P., Ding, W.	Model Checkers in Software Testing	NISTIR 6777	2/1/2002

The primary focus of formal methods is static analysis of specifications and code, but there is also a long tradition of exploiting formal methods for testing. This paper continues this model by exploring the role of model checkers in software testing. Model checkers were originally developed to check that state machines conformed to specifications expressed in a temporal logic. We show how to apply these powerful computation engines to the problems of test generation and test evaluation for a variety of test coverage criteria defined on model-based specifications.

Black, P.E., Kuhn, D.R., Williams,	Quantum Computing and	Advances in Computers (Academic Press)

In this article, we review quantum computing and communications, current status, algorithms, and problems that remain to be solved. Section 2 gives the reader a narrative tutorial on quantum effects and major theorems of quantum mechanics. Section 3 presents the “Dirac” or “ket” notation for quantum mechanics and mathematically restates many of the examples and results of the preceding section. Section 4 introduces the computer science notion of complexity and explains some quantum computing algorithms, such as Shor’s for factoring and Grover’s for searching, and error correcting schemes. Section 5 treats quantum communication and cryptography. We end with an overview of physical implementations in Section 6.

Blackburn, M., Busser, R., Nauman, A., Chandramouli, R.	Interface-Driven Model-Based Generation of Java Test Drivers	2002 Quality Week Conference, San Francisco, California

This paper extends prior work in model-based verification and describes interface-driven analysis that combines with a requirement model to support automated generation of Java test scripts. It describes concepts of models and test driver mappings using examples for testing security functionality of an Oracle database using Java and Structured Query Language(SQL) test drivers. Although the modeling and testing are focused on database security capabilities, the described concepts can be applied to develop test drivers for many other products.

Boettinger, W.J., McFadden, G.B., Warren, J., Guyer, J.E.	Model of Electrochemical "Double Layer" Using the Phase Field Method	Accepted by MRS Proceedings

We present the first application of phase field modeling to electrochemistry. A free energy functional that includes the electrostatic effect of charged particles leads to rich interactions between concentration, electrostatic potential, and phase stability. The present model, explored only for equilibrium, stationary interface, properly predicts the charge separation associated with the equilibrium double layer at the electrochemical interface and its extent in the electrolyte as a function of electrolyte concentration, as well as the form expected of electrocapillary curves.

Boggs, P.T., Kearsley, A.J., Tolle,	Optimality Conditions for Hierarchical Control	NISTIR 6898	

As part of the study of techniques for solving PDE-constrained optimization problems, we consider the approximate pointwise control of a linear parabolic system with multiple targets. Assuming a hierarchy among the objectives, we derive optimality conditions for a particular test problem and provide numerical results.

Boisvert, R.F., Pozo, R.	Java	Handbook of Accuracy and Reliability in Scientific Computing	

Our goal here is to provide to non-Java programmers some guidance as to whether Java might be appropriate for scientific applications. We will discuss some of Java’s features which promote the safety, reliability, and portability, and then briefly address the biggest concern of most scientific users: performance. We conclude with a short discussion some deficiencies of

Bouldin, C.E., Sims, J.S., Hung, H.K., Rehr, J.J., Ankudinov, A.	Parallel Calculation of Electron Multiple Scattering Using Lanczos Algorithms	Accepted by Physical Review B	

Real space multiple scattering calculations of the elctronic density of states and x-ray spectra in solids typically scale as the cube of the system and basis set size, and hence are highly demanding computationally. For example, calculations near the Si K-edge require clusters of order 103 atoms with s, p, and d states to converge adequately, and hence ~ 100 inversions of 9000

Burr, W., Hash, J.	Techniques for System and Data	ITL Bulletin, April 2002	4/18/2002

The key asset in Federal agencies today is the information and data used to implement, sustain and maintain critical government programs and operations. Current efforts in ensuring that the United States can recover and restore activities which have great impact on the physical and economic health and safety of the American public are dependent upon the ability to quickly reinstate information systems and the data required to run those systems. Effective Homeland security is dependent upon an extensive amount of corroboration and data sharing. It is essential that those managing information technology (IT) security programs ensure that they have put contingencies in place for quick restoration of IT resources. A Business Impact Analysis should be completed. As part of this process, mission critical operations should be identified along with the supporting data and systems. Subsequent to identification of these critical assets, methods for recovery of data and systems due to error or attack must be included in the overall Business Continuity Plan. This ITL Bulletin focuses on techniques for addressing this important component of contingency planning. The intent is to provide users with a quick reference primer

Carasso, A.S., Bright, D.S., Vladar, A.E.	The APEX Method and Real-Time Blind Deconvolution of Scanning Electron Microscope Imagery	NISTIR 6835 and submitted to Optical Engineering	11/28/2001

Loss of resolution due to image blurring is a major concern in electron microscopy. The point spread function describing that blur is generally unknown. This paper discusses the use of a recently developed FFT-based direct blind deconvolution procedure, the APEX method, that can process 512 x 512 images in less than a minute on current desktop platforms. The method is predicated on a restricted but significant class of shift-invariant blurs, consisting of finite convolution products of Levy probability density functions. Such blurs considerably generalize Gaussian and Lorentzian point spread functions. In this paper, the method is successfully applied to a wide variety of original SEM micrographs. Quantitative sharpness analysis of ‘ideal sample’ micrographs, shows that APEX processing can produce sharper imagery than is achievable with optimal microscope settings.

Carnahan, L.J., Rosenthal, L.S.	Healthcare Information Standards & Testing: A Concept Paper	White paper for web (http://www.nist.gov/healthcare)	9/25/2002

This paper was inspired by preliminary discussions between NIST and members of the healthcare community who are impacted by the use of emerging information technology. Topics of discussion included the current state of standards work in the healthcare community, the requirements for security, information assurance and continuity-of-operations, as well as the critical need for information interoperability to provide healthcare information and clinical care. Participants of the recently held NIST Workshop, Information Technologies for Healthcare: Barriers to Implementation, reiterated these same topics. Throughout a major theme has emerged – the plethora of healthcare standards and the need for conformance tests and testing programs. This initial paper focuses on options for analyzing, defining, and organizing appropriate standards for the healthcare community and the issues surrounding conformance testing. Further studies and discussions may uncover more information regarding other issues and challenges facing the healthcare industry and its segments, including, but not limited to, security, user interfaces, information retrieval, pervasive computing technologies and networking. These issues could then foster opportunities that allow NIST to work collaboratively with the healthcare industry to address the challenges that arise.

Chandramouli, R.	A Multi-Faceted Approach for Development of Security Architectures for Application Systems	Third Annual International Systems Security Engineering Association Conference, Orlando, Florida,	

		March 13-15, 2002

Secure application systems are often built using the Software Architecture of the system as a blue print. The Software Architecture of any application system contains along with other functional requirements, the security service requirements for the various constituent components. However for continued maintenance of the security worthiness of the application and for facilitating security re-evaluations and certifications, a separate security architecture definition for an application is also required. In this paper we describe a methodology for developing and maintaining a security-focused architecture for any application system. We have termed this architecture as the Functional Security Architectures (FSA) and the methodology as MDFSA (the acronym standing for Methodology for Development of Functional Security Architecture). FSA provides security service definitions for the various components in the Software Architecture based on abstract models. MDFSA employs a multi-faceted approach for developing the FSA – Business Process Analysis, Abstract Models of Protection & Security Service definition, Information Security Architecture, Structured Security Specification frameworks (e.g. ISO/IEC 15408 Protection Profiles/Security Target) etc. The MDFSA methodology is illustrated by using an Admissions Discharge and Transfer System, a key healthcare IT application system.

Chandramouli, R.	Enterprise Access Control Frameworks Using RBAC and XML Technologies	Book chapter in “Role-based Access Control and its Applications” by Artech Book House

In this chapter, we show that we can develop an Enterprise Access Control Framework using Role-based Access Control (RBAC) and Extensible Markup Language (XML) technologies. In the first section, we outline the general requirements for the Enterprise Access Control Model (EAM) and describe as to how RBAC meets those requirements. We call the resultant RBAC model as the “Enterprise RBAC Model”. In the second section we briefly outline the facilities that XML technologies provides for specification and processing of structured data. The meat of this chapter is in the third section where a detailed description of the development of an Enterprise RBAC Model for a commercial bank is provided using one of the XML schema languages called the “XML Schema”. In the rest of the sections we illustrate as to how XML APIs and toolsets can be utilized to perform tasks of validating the enterprise access control data in the XML document for conformance to the specification of the Enterprise RBAC Model and for mapping this data into different formats required by the access control modules in platforms hosting the various

Chandramouli, R., Blackburn, M.	Security Functional Testing Using an Interface-Driven Model-based Test Automation Approach	18th Annual Computer Security Applications Conference (ACSAC), Las Vegas, Nevada, December 9-13, 2002

Independent security functional testing on a product occupies a backseat in traditional security evaluation because of the cost and stringent coverage requirements. In this paper we present the details of an approach we have developed to automate security functional testing. The underlying framework is called TAF (Test Automation Framework) and the toolkit we have developed based on TAF we call it as TAF-SFT toolkit. The TAF-SFT toolkit uses the text-based specification of security functions provided by the product vendor and the requirements of the underlying security model to develop a machine-readable specification of security functions using the SCR (Software Cost Reduction) formal language. The resultant behavioral specification model is then processed through the TAF-SFT Toolkit to generate test vectors. The behavioral model and the test vectors are then combined with product interface specifications to automatically generate test drivers (test execution code). We illustrate the application of TAF-SFT toolkit for security functional of a commercial DBMS product. We also discuss the advantages and disadvantages of using TAF-SFT toolkit for security functional testing and the scenarios under which you

Chernick, C.M.	Federal S/MIME V3 Client Profile	NIST SP 800-49 (http://csrc.nist.gov/publications/nistpubs/index.html)

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a set of specifications for securing electronic mail. S/MIME is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s). The S/MIME specifications were designed to promote interoperable secure electronic mail, such that two compliant implementations would be able to communicate securely with one another. However, implementations may support different optional services, and the specifications may unintentionally allow multiple interpretations. As a result, different implementations of S/MIME may not be fully interoperable or provide the desired level of security. The S/MIME specifications rely on cryptographic mechanisms and public key infrastructures (PKI) to provide security services. If the cryptographic and PKI components that are used to support the S/MIME implementation are sufficiently robust, users can obtain additional assurance that sufficiently strong cryptographic algorithms are used, and that procedures are in place to protect sensitive information. Conformance to this profile helps to assure that S/MIME implementations will be able to interoperate and provide reasonable assurance to users. NIST has developed this S/MIME client profile as guidance in the development and procurement of commercial-off-the-shelf (COTS) S/MIME-compliant products. This profile identifies requirements for a secure and interoperable S/MIME V3 client implementation. (S/MIME Version 3 is the latest version of S/MIME.)

Choquette, S.J., O'Neal, L.E., Duewer, D.L., Filliben, J.J.	Rare Earth Glass Reference Materials for Near Infrared Spectrometry: Sources of X-Axis Location Variability	Analytical Chemistry

The National Institute of Standards and Technology recently introduced two optical filter standards for wavelength/wavenumber calibration of Near-Infrared (NIR) spectrometers. Standard Reference Materials (SRMs) 2035 and 2065 were fabricated in lots of ~100 units each from separate melts of nominally identical rare-earth glass. Since individual filter certification is extremely time-consuming and thus costly, reasonably economic production of these SRMs required the ability to batch certify band locations. Given the band location precision specification of ~0.2 cm-1, rigorous evaluation of material heterogeneity was required to demonstrate the adequacy of batch certification for these materials. Among-filter variation in measured band locations convolves any influence of material heterogeneity with those of environmental, procedural, and instrument artifacts. While univariate analysis of variance established band-specific heterogeneity upper bounds, it did not provide quantitative descriptions of the other possible sources for the observed measurement variance. Abstract factor analysis enabled both the identification and isolation of the principle NIR band location variances among the SRM 2065 filters. After correction for these variance sources, the upper bound on the material heterogeneity was determined to be 0.03 cm-1 for all bands. Since this is a small component of the measurement uncertainty, we conclude that batch analysis provides an acceptable certification approach for these and similarly fabricated rare-earth glass reference materials.

Coakley, K.J., Splett, J.D., Janezic, M.D., Kaiser, R.F.	Estimation of Q-Factors and Resonant Frequencies	IEEE Transactions on Microwave Theory and Techniques

We estimate the quality factor Q and resonant frequency f0 of a microwave cavity based on resonance curve observations on an equally-spaced frequency grid. The observed resonance curve is the squared magnitude of an observed complex scattering parameter. We characterize the variance of the additive noise in the observed resonance curve parametrically. Based on this noise characterization, we estimate Q and f0 and other associated model parameters by the method of weighted least squares (WLS). Based on asymptotic statistical theory, we also estimate the one-sigma uncertainty of Q and f0. In a simulation study, the WLS method outperforms the 3-dB method and the Estin method. For real data, we show that the WLS method yields the most precise estimates. Given that the resonance curve is sampled at a fixed number of equally-spaced frequencies in the neighborhood of the resonant frequency, we determine the optimal frequency spacing in order to minimize the asymptotic

Coakley, K.J., Wang C.-M., Hale, P.D., Clement, T.S.	Adaptive Characterization of Jitter Noise in Sampled High-Speed Signals	IEEE Transactions on Instrumentation and Measurement

We estimate the root-mean-square (RMS) value of timing jitter noise in simulated signals similar to measured high-speed sampled signals. The simulated signals are contaminated by additive noise, timing jitter noise, and time shift errors. Before estimating the RMS value of the jitter noise, we align the signals (unless there are no time shift errors) based on estimates of the relative shifts from cross-correlation analysis. We compute the mean and sample variance of the aligned signals based on repeated measurements at each time sample. We estimate the derivative of the average of the aligned signals at each time sample based on a regression spline model. Our estimate of the RMS value of the jitter noise depends on estimated derivatives and sample variances at time samples where the magnitude of the estimated derivative exceeds a selected threshold. Our estimate is generally biased. Using a parametric bootstrap approach, we adaptively adjust the estimate based on an estimate of this bias. We apply our method to real data collected at NIST. We study how results depend on the derivative threshold.

Cugini, J.V.	Information Access: Do You Mind?	NIST SP 990, Measuring the Performance and Intelligence of Systems: Proceedings of the 2002 PerMIS Workshop

Successful execution of many information-based tasks depends crucially on contextual knowledge. Language processing is particularly sensitive to context, and I will concentrate on it in this extended abstract as the example par excellence of knowledge-dependent information access.

Cugini, J.V.	TreeDec: An Annotation Tool to Support Website Navigation	Internetworking, a Publication of the Internet Technical Group of the Human Factors & Ergonomics

Websites are often organized into logical hierarchies, or tree structures, in order to help users navigate. Ideally, users could view the entire tree, or jump to nearby pages. TreeDec (= Tree Decorator) is a system to support website authors and maintainers by providing automatic annotation of webpages under the control of a central file that represents the tree structure.

Cypher, D.E.	IEEE 802.11 and Bluetooth, Will They or Won't They?	Institute of Electrical and Electronics Engineers (IEEE)

This paper provides information on the IEEE 802.11 standard and some of its extensions and the Bluetooth™ wireless technology, and attempts to provide an answer(s) to the question that is plaguing the 2.4 GHz frequency band usage community. That question is, Will the IEEE 802.11 and the Bluetooth wireless technologies function when the other is present? The answer(s) provided here are based on both an analysis of the protocols and measurement experiments. Since the 2.4 GHz frequency band is an unlicensed band, there is no controlling body for the development of protocols for equipment that use it. The Federal Communication Commission (FCC) only provides regulatory issues on power and usage for the United States of America. Other countries have similar regulatory bodies. With this lack of coordination, it is not surprising that this situation occurs, but what happens when an international standards organization, like the IEEE, builds multiple independent systems that use the same frequency band? Other questions also exist on the subject, like: Is there a need for another wireless technology within the same frequency band? Are the technologies in competition with one another? or should these technologies

Dabrowski, C.E., Mills, K.L.	Adaptive Jitter Control for UPnP	2003 International Conference on Communications

Selected service-discovery systems allow clients to issue multicast queries to locate network devices and services. Qualifying devices and services respond directly to clients; thus, in a large network, potential exists for responses to implode on a client, overrunning available resources. To limit implosion, one service-discovery system, UPnP, permits clients to include a jitter bound in multicast (M-Search) queries. Qualifying devices use the jitter bound to randomize their responses. Initially, clients lack sufficient knowledge to select an appropriate jitter bound, which varies with network size. In this paper, we characterize the performance of UPnP M-Search for various combinations of jitter bound and network size. In addition, we evaluate the performance and costs of four algorithms that might be used for adaptive jitter control. Finally, we suggest an alternative to

Dabrowski, C.E., Mills, K.L., Elder,	Understanding Consistency Maintenance in Service Discovery Architectures during Communication	Proceedings of the Third International Workshop on Software Performance (WOSP 2002)

Current trends suggest future software systems will comprise collections of components that combine and recombine dynamically in reaction to changing conditions. Service-discovery protocols, which enable software components to locate available software services and to adapt to changing system topology, provide one foundation for such dynamic behavior. Emerging discovery protocols specify alternative architectures and behaviors, which motivate a rigorous investigation of the properties underlying their designs. Here, we assess the ability of selected designs for service-discovery protocols to maintain consistency in a distributed system during catastrophic communication failure. We use an architectural-description language, called Rapide, to model two different architectures (two-party and three-party) and two different consistency-maintenance mechanisms (polling and notification). We use our models to investigate performance differences among combinations of architecture and consistency maintenance mechanism as interface-failure rate increases. We measure system performance along three dimensions: (1) update responsiveness (How much latency is required to propagate changes?), (2) update effectiveness (What is the probability that a node receives a change?), and (3) update efficiency (How many messages must be sent to propagate a change throughout the topology?). We use Rapide to understand how failure-recovery strategies contribute to differences in performance. We also recommend improvements to architectural-description languages.

Dabrowski, C.E., Mills, K.L., Elder,

Understanding Consistency Maintenance in Service Discovery Architectures in Response to Message

Proceedings of the 4th International Workshop on Active Middleware Services

Current trends suggest future software systems will comprise collections of components that combine and recombine dynamically in reaction to changing conditions. Service-discovery protocols, which enable software components to locate available software services and to adapt to changing system topology, provide one foundation for such dynamic behavior. Emerging discovery protocols specify alternative architectures and behaviors, which motivate a rigorous investigation of the properties underlying their designs. Here, we assess the ability of selected designs for service-discovery protocols to maintain consistency in a distributed system during severe message loss. We use an architecture description language, called Rapide, to model two different architectures (two-party and three-party) and two different consistency-maintenance mechanisms (polling and notification). We use our models to investigate performance differences among combinations of architecture and consistency-maintenance mechanism as message-loss rate increases. We measure system performance along three dimensions: (1) update responsiveness (How much latency is required to propagate changes?), (2) update effectiveness (What is the probability that a node receives a change?), and (3) update efficiency (How many messages must be sent to propagate a change throughout the topology?).

Dao, N., Ross, C.A., Castano, F.J., Donahue, M.J., Whittenburg,

Micromagnetics Simulation of Asymmetric Pseudo-Spin Valve Dots

Proceedings of the 2002 Materials Research Society Spring Meeting, San Francisco, California, April 1-5, 2002

We present our recent simulation results for Ni79Fe21 (5 nm)/Cu (3 nm)/Co (4nm) pseudo-spin valves. These simulations have been conducted on several different aspect ratios of rectangular dots. Distinct switches of the two magnetic layers were observed. At smaller aspect ratios, magnetization reversal proceeds through a leaf state in the soft layer and a flower state in the hard layer. For larger aspect ratios, reversal proceeds by nucleation and annihilation of a domain wall. Our simulations show a reasonable agreement with the experimental results. Differences between the experimental and simulation results are

Devaney, J.E., Hagedorn, J.G.

The Role of Genetic Programming in Describing the Microscopic Structure of Hydrating Plaster

Late Breaking Papers in Genetic and Evolutionary Computation Conference, GECCO-2002, New York, N.Y., July 8-13, 2002

7/8/2002

We apply genetic programming in conjunction with other machine learning methods to obtain concise rules that accurately identify scientifically meaningful components in hydrating plaster over multiple time periods. Genetic programming enables the derivation of understandable rules from otherwise opaque classifications. Our study was based on three dimensional data obtained through X-ray microtomography at five times in the hydration process. Starting with statistics based on locality and output from an unsupervised classification system (autoclass), we use genetic programming to derive simple rules for identifying three classes. These rules are tested on a separate subset of the plaster datasets that had been labeled with their autoclass predictions. The rules were found to have both high sensitivity and high positive predictive value.Genetic programming in conjunction with other machine learning methods enabled us to go from unlabeled datato simple classification rules in a

Dienstfrey, A., Huang, J.	Integral Representations for Elliptic Functions	Submitted to Transactions of the American Mathematical Society

We derive integral representations for classical objects arising in the theory of elliptic functions: the Eisenstein series, and Weiertrass' $\wp$ and ζ functions. The derivations proceed from the Laplace-Mellin transformation for multipoles, and an elementary lemma on the summation of 2D geometric series. In addition, we present new results concerning the continuation of the Eisenstein series to an entire function in the complex plane --- $E_n\to \widetilde{E}_s, s\in {\bf C}$ --- and the value of the conditionally convergent series, denoted by $\widetilde{E}_2$ below, as a function of summation over increasingly large

Donahue, M.J., Porter, D.G.	Analysis of Switching in Uniformly Magnetized Bodies	IEEE Transactions on Magnetics

A full analysis of magnetization reversal of a uniformly magnetized particle by coherent rotation is presented. The magnetization energy of the particle in the presence of an applied field H is modeled as E = (μ0/2)MT DM - μ0HTM.This model includes shape anisotropy, any number of uniaxial anisotropies, and any energy that can be represented by an effective field that is a linear function of the uniform magnetization M. The model is a generalization to three dimensions of the Stoner-Wohlfarth model. Lagrange multiplier analysis leads to quadratically convergent iterative algorithms for computation of switching field, coercive field, and the stable magnetization(s) of the particle in the presence of any applied field. Magnetization dynamics are examined as the applied field magnitude |H| approaches the switching field Hs, and it is found that the precession frequency f a (Hs -

Donahue, M.J., Vértesy G., Pardavi-Horvath, M.	Defect Related Switching Field Reduction in Small Magnetic Particle	Journal of Applied Physics

An array of 42 µm square, 3 µm thick garnet particles has been studied. The strong crystalline uniaxial anisotropy of these particles results in the stable remanent state being single domain with magnetization parallel to the film normal. Magnetooptic measurements of individual particles provide distribution statistics for the easy-axis switching field Hsw, and the in-plane hard-axis effective anisotropy field, Heff, which induces the formation of a metastable stripe domain structure. Both Hsw and Heff are much smaller than the crystalline anisotropy field. Micromagnetic simulations show that the small Hsw cannot be attributed to shape anisotropy, but is consistent with smooth, localized reductions in the crystalline anisotropy caused by

Dray, J., Schwarzhoff, T.	Overview: The Government Smart Card Interoperability Specification	ITL Bulletin, July 2002	7/18/2002

This ITL Bulletin summarizes the Government Smart Card Interoperability Specification, which provides solutions to a number of the interoperability problems associated with smart card technology.

Dray, J.F., Goldfine, A., Iorga, M., Schwarzhoff, T., Wack, J.	Government Smart Card Interoperability Specification	NISTIR 6887	6/28/2002

Many organizations recognize the importance of smart card technology and wish to take advantage of this technology to strengthen the security of authentication and access control processes. However, widespread deployment of smart cards in the U.S. has been hampered by a lack of interoperability standards. This Government Smart Card Interoperability Specification(GSC-IS) defines a comprehensive architectural framework for smart card interoperability. The GSC-IS framework establishes a common smart card service provider model that allows applications programmers to access smart card services without regard for the underlying implementation details. The GSC-IS was developed by the Government Smart Card Interagency Advisory Board, a joint committee of federal agencies and industry partners in conjunction with the General Service

Duff, I.S., Heroux, M.A., Pozo, R.	An Overview of the Sparse Basic Linear Algebra Subprograms: The New Standard from the BLAS Technical	ACM Transactions on Mathematical Software	

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 standard is 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.

Dworkin, M.	Recommendation for Block Cipher Modes of Operation Methods and	NIST SP 800-38A (http://csrc.nist.gov/publications/nistpubs/index.html)	12/10/2001

This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). Used with an underlying block cipher algorithm that is approved in a Federal Information Processing Standard (FIPS), these modes can provide cryptographic protection for sensitive, but unclassified, computer data.

Fabijonas, B.R., Lozier, D.W., Olver, F.W.J.	Algorithm xxx: Airy Functions	Association for Computing Transactions on Mathematical Software	

We present a Fortran 90 module which computes the solutions of Airy's differential equation, and their derivatives, both on the real line and in the complex plane. The computational methods are numerical integration of the differential equation and summation of asymptotic expansions for large argument. The module also computes the zeros and associated values of the solutions and their derivatives, and modulus and phase functions on the negative real axis.

Filliben, J.J., Gurley, K., Pinelli, J.P., Simiu, E., Subramanian, M.	Fragility Curves, Damage Matrices, and Wind-Induced Loss Estimation	Conference on Risk Analysis	

This note presents a conceptual framework for the definition of basic damage states and of the corresponding fragility curves and conditional probabilities, and its use for the estimation of damage matrices. The framework is designed with two considerations in mind. First, losses due to multiple types of damage are calculated so that no type of damage is counted more than once, no type of possible damage is omitted from the calculations, and all interactions between various types of damage are accounted for. Damage is included that may vary continuously as a function of wind speed but is discretized for computational purposes. Second, the losses are calculated by correctly accounting for the dependence between various damage states (e.g., window breakage and roof uplift). The note also discusses the use of damage matrices for the estimation of expected losses due to a windstorm event, of expected annual losses, and of measures of uncertainty pertaining to expected losses, both at a specified location and over a larger geographical area. The framework developed in the paper is illustrated for the conceptually simple case of two basic damage states. Work is in progress on the application of the framework to various types of structures involving larger numbers of basic damage states with various mutual dependence and damage sequence scenarios. Work is also in progress on the estimation of uncertainties in loss calculations, based on certainties in the estimation of fragility curves, associated conditional probabilities, and hurricane wind speeds. One of the applications of our work is the development of vulnerability curves and associated uncertainty measures for cases where comprehensive loss data from which such curves may be developed are not available.

Fisher, G.E.	Computer Forensics Guidance	ITL Bulletin, November 2001	11/15/2001

This ITL Bulletin describes two projects in the computer forensics arena and provides guidance on the use of the products developed from them. The first project, the National Software Reference Library (NSRL), describes a database of known file “fingerprints” for use in investigations of crimes that involve computers. The second, the Computer Forensics Tool Testing (CFTT) project, describes ongoing work in the development of specifications and test methods for testing automated computer

Fong, E., Ivezic, N., Korchak, R., Peng, Y., Rhodes, T.	Agent Technology: Feasibility for Business and Manufacturing Application	NISTIR 6858	3/1/2002

Electronic commerce (e-commerce) may be defined as the entire set of processes that support transaction activities on a network and involve information analysis. These activities spawn product information and display events, services, providers, consumers, advertisers, support for transactions, brokering systems for a variety of services and actions (e.g., finding certain products, finding cheaply priced products, etc.) The potential of agent-based systems has not been realized yet, in part, because of the lack of understanding how the agent technology support business-to-business e-commerce processes. This report is to investigate the current state of agent technology and the feasibility of applying agent-based computing to

Franiatte, J.C., Satterfield, S.G., Bryant, G.W., Devaney, J.E.	Parallelization and Visualization of Computational Nanotechnology LCAO Method	Nanotechnology at the Interface of Information Technology, New Orleans, Louisiana, February 7-9, 2002	

Accurate atomic-scale quantum theory of nanostructures and nanosystems fabricated from nanostructures enables precision metrology of these nanosystems and provides the predictive, precision modeling tools needed for engineering these systems for applications including advanced semiconductor lasers and detectors, single photon sources and detectors, biosensors, and nanoarchitectures for quantum coherent technologies such as quantum computing. The tight-binding model based upon the Linear Combination of Atomic Orbitals (LCAO) method provides an atomistic theory for nanostructures which is accurate and easy to implement(1). The tight-binding method is ideal for modeling small nanostructures. However, the method becomes impractical to use on sequential computers, due to long run times, for modeling nanostructures with more than 25,000 atoms. Dramatic improvements in run time can be achieved through parallelization. We parallelize this method by dividing the structure into layers. Communication is across layers. First we create the structure. Then we solve the Hamiltonian equation for each atom considering only nearest neighbors using PARPACK(2). This parallel implementation is nearly linear in time. The output of the code is transferred to the NIST immersive environment where we study the structure interactively. This provides us with a detailed inspection and visualization of the structures and the atomic scale variation of calculated nanostructure properties that is not possible with any static graphical representation. We save the interaction with the structure in the immersive environment as a quicktime movie. The parallel implementation can handle arbitrary nanostructure shapes through an input file specification procedure. Structures of up to one million atoms are currently being studied. (1) G. W. Bryant and W. Jaskolski, Physica E 11, 72 (2001). (2) K. Maschhoff, D. Sorensen, "A portable implementation of ARPACK for distributed memory parallel architectures", Preliminary proceedings, Copper Mountain Conference on Iterative Methods, 1996.

Galtier, V., Mills, K.L., Carlinet, Y.	Modeling CPU Demand in Heterogeneous Active Networks	Proceedings of the DARPA Active Networks Conference and Exposition, June 2002

Active-network technology envisions deployment of virtual execution environments within network elements, such as switches and routers. As a result, application-specific processing can be applied to network traffic. To use such technology safely and efficiently, individual nodes must provide mechanisms to manage resource use. This implies that each node must understand the varying resource demands associated with specific network traffic. Well-accepted metrics exist for expressing bandwidth (bits per second) and memory (bytes) in units independent of the capabilities of particular nodes. Unfortunately, no well-accepted metric exists to express processing (i.e., CPU time) demands in a platform-independent form. This paper describes and evaluates an approach to model the CPU demand of active packets in a form that can be interpreted among heterogeneous nodes in an active network. The paper applies the model in two applications: (1) controlling CPU use and (2) predicting CPU demand in an active-network node. The model yields improved performance when compared against the approach currently used in many active-network execution environments. The paper also discusses the limits of the proposed

Garofolo, J.S.	Using Speech Technologies for Information Access: Does it Require Getting Involved in Mechanisms of Mind and Intelligence?	NIST SP 990, Measuring the Performance and Intelligence of Systems: Proceedings of the 2002 PerMIS Workshop

Speech is arguably man's oldest and most natural form of communication. Speech and language are also inextricably linked to human thought and intelligence. Therefore, the recognition and understanding of spoken and written language was from the beginning an important component of artificial intelligence research. Initial efforts at speech recognition using classic AI techniques were thought to have failed because of the computational limitationss of the time. Yet, even with the major advances that have occurred in computing power over the last decade, successful communication with machines using human

Garris, M.D.	Recommendation for Interstate Criminal History Transmission	NISTIR 6820	11/1/2001

This report contains technical comments and recommendations regarding the "Interstate Criminal History Transmission Specification - XML Version 2.01" published June 2001. This specification was written by a national task force, the Joint Task Force on Rap Sheet Standardization (JTF), composed of members representing federal, state, and local criminal justice agencies. The Federal Bureau of Investigation (FBI) presented the National Institute of Standards and Technology (NIST) with of copy of the JTF's specification and requested an independent review and comment. Upon technical review, NIST determined that the JTF's published XML schema was out of date with current standards. It was also observed that the published schema was developed using a single validating parser. NIST discovered that the same schema failed to work when used by a different parser written to the same schema standards. From these discoveries, NIST set out to revise the JTF's published schema, rap sheet, and stylesheet in an effort to bring them up to current standards and demonstrate their interoperability with a variety of tools. NIST was successful in achieving these objectives, and revised files are provided in the appendices. This report describes the technical issues raised and the solutions implemented in the process of achieving these objectives.

Gentile, C., Sznaier, M.	Hyperborders in the Voronoi-Diagram-Based Neural Net for	Int. Joint Conf. on Neural Networks, Honolulu, HI, May 12-17,	

We propose a neural network to answer a point query in Rn partitioned based on the Voronoi diagram. Our novel design offers the potential to reduce both the number of neurons and connection weights of previous designs, employing a cost function which enables a tradeoff between the two to suit a specific implementation. Our simplified structure requires neither delay weights nor complex neurons, while retaining the main advantage of previous designs to furnish precise values for the neurons and connection weights, as opposed to trial and error iterations or ad-hoc parameters.

Gentile, C., Sznaier, M.	An Improved Voronoi-Diagram-Based Neural Net for Pattern Classification	IEEE Transactions on Neural Networks, Vol. 12, No. 5, September 2001	

In this brief paper, we propose a novel two-layer neural network to answer a point query in Rn which is partitioned into polyhedral regions. Such a task solves among others nearest neighbor clustering. As in previous approaches to the problem, our design is based on the use of Voronoi diagrams. However our approach results in substantial reduction of the number of neurons, completely eliminating the second layer, at the price of requiring only two additional clock steps. In addition, the design process is also simplified while retaining the main advantage of the approach, namely its ability to furnish precise values for the number of neurons and the connection weights necessitating neither trial and error type iterations nor ad hoc parameters.

Gentile, C., Sznaier, M., Camps, O.	Segmentation for Robust Tracking in the Presence of Severe Occlusion	IEEE International Conference on Computer Vision and Pattern Recognition, Kauai, Hawaii, Dec. 9-14, 2001

Tracking an object in a sequence of images can fail due to partial occlusion or clutter. Robustness can be increased by tracking a set of “parts”, provided that a suitable set can be identified. In this paper we propose a novel segmentation, specifically designed to improve robustness against occlusion in the context of tracking. The main result shows that tracking the parts resulting from this segmentation outperforms both tracking parts obtained through traditional segmentations, and tracking the entire target. Additional results include a statistical analysis of the correlation between features of a part and tracking error, and identifying a cost function highly correlated with the tracking error.

Gentile, C., Van Dyck, R.E.	Kinetic Spanning Trees for Minimum-Power Routing in MANETS	IEEE Vehicular Technology Conference, Birmingham, Alabama, May 6-9, 2002

A distributed kinetic spanning tree algorithm is proposed for routing in wireless mobile ad hoc networks. Assuming a piecewise linear motion model for the nodes, the sequence of shortest-path spanning trees is determined, valid until the time of the next node trajectory change. By computing the sequence of trees using one execution of the distributed routing algorithm, in contrast to computing the tree for a single time instant, the number of routing messages is substantially reduced. Moreover, the total power required to route through the trees as a function of time is also lower.

George, W.L., Scott, J.	Screen Saver Science: Realizing Distributed Parallel Computing with Jini and JavaSpaces	The Eleventh International Conference on Parallel Architectures and Compilation

We describe an experimental distributed parallel programming environment, Screen Saver Science (SSS), that utilizes a network of otherwise idle processors as the compute nodes. This environment is built on top of the Java/Jini/JavaSpaces technology to provide a robust and scalable system with a minimum of additional software required. Unlike other existing distributed computing environments, such as SETI@Home, SSS allows the compute nodes to communicate with each other during the computation rather than communicating only with a central control system. Also, the compute nodes can submit tasks to the system as well as take tasks to execute. Using SSS, we intend to explore the expanded space of distributed parallel algorithms made possible

Gharavi, H.	Video Transmission for Third Generation Mobile Communication Systems	Milcom 2001, McLean, Virginia, October 28-31, 2001	10/28/2001

This paper presents a method of transmitting video over the cdma2000 mobile systems. In this method, the video bit-stream, after splitting, is transmitted via the supplemental channels of the cdma2000 reverse link. The method takes advantage of the direct spread multiplexing structure of the supplemental channels to transmit divided video at differing priority classes. This is accomplished by adopting the relative gain adjustment strategy where the most error sensitive video information is transmitted via a channel with higher power. The most challenging aspect of this investigation has been to maintain full compatibility with the cdma2000 standard. In particular, for the reverse link where the power allocation is tightly controlled, this strategy has been successfully deployed by taking advantage of the flexibility of its link budget. Finally, we will demonstrate that this strategy can result in a significantly higher quality of the reconstructed video data when transmitted over time-varying multipath fading

Gharavi, H.	Pilot Assisted 16-level QAM for Wireless Video	IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 2, February 2002	2/1/2002

This paper presents a twin-class transmission system for narrowband radio access channels suitable for handheld video phone and multimedia portable PC applications. The transmission system is comprised of a hierarchical 16-QAM modulation technique and a channel-coding scheme. The formation of dual-priority transmission is due to differing error resiliencies of the bits that make up a given symbol in a Gray-coded 16-QAM. On this basis, a twin-class pilot-assisted fade-estimation technique that can gracefully reduce the power loss caused by the transmission of pilot overhead is developed. The twin-class 16-QAM system is then used to transport a compressed video bitstream, which is partitioned to match the bit-error sensitivity of the transmitted symbol. The partitioning scheme is based on a separation of the variable-length (VL) coded discrete cosine transform (DCT) coefficients within each DCT block. This partitioning scheme is then applied to split the ITU-T H.263-coded bitstream. The scheme is suitable for constant bit-rate transmission (CBR), where the fraction of bits assigned to each of the two partitions can be adjusted according to the requirements of the unequal error protection scheme employed. The distribution of the VL-coded (VLC) information amongst the two partitions is performed adaptively. Finally, the performance of the partitioning scheme for transmission of video signals using our twin-class 16-QAM trans-mission system is evaluated under multipath fading conditions.

Gharavi, H., Ban, K.	Video Communications Via Multihop Ad-Hoc Networks: Design and	Conference Proceedings: 3Gwireless’2002 Conference, San Francisco, California, May 31, 2002	5/31/2002

This paper presents the design and implementation of a mobile ad-hoc network for video communications. The network architecture is based on cluster-to-cluster operation using IEEE 802.11b FHSS (Frequency Hopping Spread Spectrum). FHSS is considered to provide a better network scalability in terms of area coverage. In this architecture, the participating nodes in one cluster communicate with nodes in other clusters via their respective mobile Access-Points (APs). The link between the mobile APs is accomplished using the Ad-hoc On-demand Distance Vector (AODV) routing protocol. Video streaming is based on H.263+/RTP/UDP/IP/802.11.b. This network has been implemented using a set of APs and PDAs devices for demonstration and field testing. In our implementation so far, the experimental set up consists of 4-clusters operating in an ad-hoc manner. The paper will present the design aspects of the proposed network as well as the overall system evaluation in terms of video quality,

Gharavi, H., Reza-Alikhani, H.	A Pel-Recursive Motion Estimation Algorithm	NISTIR 6822 and IEEE Electronics Letters	

This paper presents a new pel recursive motion estimation algorithm for video coding applications. The derivation of the algorithm is based on Recursive Least-Squares (RLS) estimation that minimizes the mean square prediction error. A comparison with the modified Steepest-descent gradient estimation technique algorithm shows significant improvement in terms of mean-square prediction error performance.

Gilsinn, D.E., Cheok, G.S., O’Leary, D.P.	Reconstructing Images of Bar Codes for Construction Site Object	Proceedings of the 19th IAARC/CIB/IEEE/IFAC International Symposium on Automation and Robotics in Construction, ISARC 2002, NIST, Gaithersburg, Maryland, September 23-25, 2002	9/23/2002

This paper discusses a general approach to reconstructing ground truth intensity images of bar codes that have been distorted by LADARoptics. The first part of this paper describes the experimental data collection of several bar code images along with experimental estimates of the LADAR beam size and configuration at various distances from the source. Mathematical models of the beam size and configuration were developed and were applied through a convolution process to a simulated set of bar code images similar to the original experiment. This was done in order to estimate beam spread models (beam spread models are unique to each specific LADAR) to be used in a deconvolution process to reconstruct the original bar code images from the distorted images. In the convolution process a distorted image in vector form g is associated with a ground truth image f and each element of g is computed as a weighted average of neighboring elements of f to that associated element. The deconvolution process involves a least squares procedure that approximately solves a matrix equation of the form Hf = g where

Gilsinn, D.E., Ling, A.V.	Comparative Statistical Analysis of Test Parts Manufactured in Production Environments	NISTIR 6868	6/30/2002

Estimating error uncertainties arising in parts produced on machine tools in production machine shops is not a well understood process. The current study details a process of estimating these error uncertainties. A part with significant features was defined and a vertical turning center was selected in a production shop to make multiple copies of the part. Machine tool error components were measured using a laser ball bar instrument. Twenty-one copies of the part were produced and measured on a coordinate measuring machine. A machine tool error model based on the measurements of the vertical turning center machine tool errors was developed. Uncertainty estimates of the errors in the working volume were calculated. From coordinate measuring machine data error uncertainties at points on the part were developed. Distances between hole centers were computed and uncertainty estimates of these lengths generated. Many of the hole centers were designed to fall along orthogonal lines. Uncertainty estimates were computed of the orthogonality of these lines. All of these estimated uncertainties were compared against uncertainties computed from the measured parts. The main conclusion of the work is that the Law of Propagation of Uncertainties can be used to estimate machining uncertainties and that predicted uncertainties can be related to actual part error uncertainties.

Golmie, N., Chevrollier, N.	Techniques to Improve Bluetooth Performance in Interference	Proceedings of the 20th Military Communications Conference (MILCOM 2001), Vienna, Virginia, Oct. 28-31, 2001	10/28/2001

Bluetooth is a radio technology for Wireless Personal Area Networks operating in the 2.4 GHz ISM band. Since both Bluetooth and IEEE 802.11 devices use the same frequency band and may likely come together in a laptop or may be close together at a desktop, interference may lead to significant performance degradation. The main goal of this paper is to propose solutions to the interference problem consisting of power control adjustments and scheduling policies to be implemented by the Bluetooth device. Simulation results are given for selected scenarios and configurations of interest.

Golmie, N., Chevrollier, N., El Bakkouri, I.	Interference Aware Bluetooth Packet Scheduling	Proceedings of Globecom 2001, San Antonio, Texas, November 25-29, 2001	11/25/2001

Bluetooth is a radio technology for Wireless Personal Area Networks operating in the 2.4 GHz ISM band. Since both Bluetooth and IEEE 802.11 devices use the same frequency band and may likely come together in a laptop or may be close together at a desktop, interference may lead to significant performance degradation. The main goal of this paper is to propose a scheduling algorithm aimed at reducing the impact of interference. This algorithm takes advantage of the fact that devices in the same piconet will not be subject to the same levels of interference on all channels of the band. The basic idea is to utilize the Bluetooth frequency hopping pattern and distribute channels to devices such that to maximize their throughput while ensuring fairness of access among users. Simulation results are given for selected scenarios and configurations of interest.

Grance, T., Hash, J., Peck, S., Smith, J., Korow-Diks, K.	Security Guide for Interconnecting Information Technology Systems	NIST SP 800-47 (http://csrc.nist.gov/publications/nistpubs/index.html)	9/3/2002

The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, & terminating interconnections between information technology (IT) systems that are owned & operated by different organizations. They are consistent with the requirements specified in the Office of Management and Budget (OMB) Circular A-130, Appendix III, for system interconnection and information sharing.A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data & other information resources. The document describes benefits of interconnecting IT systems, defines the basic components of an interconnection, identifies methods & levels of interconnectivity, & discusses potential security risks.The document then presents a “life-cycle” approach for system interconnections, with an emphasis on security. Four phases are addressed:§ Planning the interconnection: the organizations perform preliminary activities; examine technical, security, & administrative issues; & form an agreement governing the management, operation, & use of the interconnection.§ Establishing the interconnection: the organizations develop & execute a plan for establishing the interconnection, including implementing or configuring security controls. § Maintaining the interconnection: the organizations maintain the interconnection after it is established to ensure that it operates properly & securely.§ Disconnecting the interconnection: one or both organizations may terminate the interconnection. The termination should be conducted in a planned manner to avoid disrupting the other party’s system. In an emergency, however, one or both organizations may choose to terminate the interconnection immediately. The document provides recommended steps for completing each phase, emphasizing security measures to protect the systems & shared data.The document also contains guides & samples for developing an Interconnection Security Agreement (ISA) & a Memorandum of Understanding/Agreement (MOU/A). The ISA specifies technical & security requirements of the interconnection; the MOU/A defines the responsibilities of the organizations. Finally, the document contains a guide for developing an Implementation Plan to establish the

Gurski, K.F., McFadden, G.B.	Modeling Quantum Wire Stability	Sigma Xi Poster (http://www.nist.gov/sigmaxi/Posters02/Gurski-abst.html)	2/6/2002

Quantum wires (alternatively called nanowires) are "one-dimensional" crystals that are grown epitaxially on a heterogeneous substrate. The wires are typically less than one nanometer high, a few nanometers wide, and can be as long as a micron. A linear stability analysis suggests that quantum wires with an isotropic surface energy would tend to bead up rather than persist as wires ("Rayleigh instability"). However, there are also several sources of anisotropy in the system, including surface tension anisotropy and elastic anisotropy associated with an elastic misfit between the wire and substrate crystal structures. To address the effects of surface tension anisotropy on the Rayleigh instability, we compute the second variation of the surface free energy of an isolated wire whose cross section is given by the associated two-dimensional equilibrium shape. We consider the case of a cubic material, and compute the stability of the wire to general perturbations when the axis of the wire is in high symmetry orientations such as [001], [011], and [111]. For small levels of anisotropy, the stability can be computed approximately via perturbation theory. For larger amplitudes of anisotropy, we have computed the stability numerically by solving an associated Sturm-Liouville eigenvalue problem. We find that surface tension anisotropy can either promote or suppress the Rayleigh instability, depending on the orientation of the wire and the magnitude and sign of the anisotropy.

Gurski, K.F., McFadden, G.B.	The Effect of Anisotropic Surface Energy on the Rayleigh Instability	NISTIR 6892 and Proceedings of the Royal Society of London,	

We determine the linear stability of a rod or wire subject to capillary forces arising from an anisotropic surface energy. The rod is assumed to be smooth with a uniform cross section given by a 2-D equilibrium shape. The stability analysis is based on computing the sign of the second variation of the surface energy, which is examined by solving an associated eigenvalue problem. The eigenproblem is a coupled pair of second-order ordinary differential equations with periodic coefficients that depend on the second derivatives of the surface energy with respect to orientation variables. We apply the analysis to examples with uniaxial or cubic anisotropy, which illustrate that anisotropic surface energy plays a significant role in establishing the stability of the rod. Both the magnitude and sign of the anisotropy determine whether the contribution stabilizes or destabilizes the system relative to the case of isotropic surface energy, which reproduces the classical Rayleigh instability.

Hagwood, C.	On the Asymptotic Distribution of Sums of Independent Nonidentically Distributed Pareto Variates	SIAM Journal of Applied	

The sum of independent Pareto random variables with varying parameters are shown to converge to a stable distribution. This extends a result of Blum for i.i.d. Pareto random variables.

Harman, D.	The Importance of Focused Evaluations: A Case Study of TREC	Proceedings of the Second NTCIR Workshop on Research in Chinese & Japanese Text Retrieval and Text Summarization (May 2000 – March 2001)	

Evaluation has always been an important part of scientific research, and in information retrieval, this evaluation has mostly been done using test collections. In 1992 a new test collection was built at the National Institute of Standards and Technology (NIST), and a focused evaluation (the Text REtrieval Conference or TREC) was started to use the collection. Results from nearly 10 years of this focused evaluation show significant technology transfer across systems, leading to major improvements in system performance. Focused evaluations also create the ability to target specific problems in language technology, such as retrieval across languages, and to design tasks for evaluation such that issues can be studied concurrently by multiple groups. This paper will discuss some of the tasks that have been examined in TREC, including critical factors in the design of those evaluations. Additionally, a new focused evaluation, the Document Understanding Conference (DUC) which will examine

Harman, D., Over, P.	The DUC Summarization Evaluations	Proceedings of HLT 2002 Second International Conference on Human Language Technology Research	

There has been a long history of research in text summarization by both the text retrieval and the natural language processing communities, but evaluation of this research has always presented problems. In 2001 NIST launched a new text summarization evaluation effort, guided by a roadmap from the research community and sponsored by the DARPA TIDES project. This paper is a report of the first formal evaluation in a new conference called the Document Understanding Conference (DUC).

Hash, J.S.	Risk Management Guidance for Information Technology Systems	ITL Bulletin, February 2002	2/28/2002

Risk Management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Organizations use risk assessment, the first step in the risk management methodology, to determine the extent of the potential threat, vulnerabilities, and the risk associated with an information technology (IT) system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, the second step of risk management, which involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems throughout their system development life cycle (SDLC). The ultimate goal is to help organizations to better manage

Herman, M.	Information Access Technology: Does It Require Getting Involved in Mechanisms of Mind and Intelligence?	NIST SP 990, Measuring the Performance and Intelligence of Systems: Proceedings of the 2002 PerMIS Workshop	

The world produces between 1 and 2 exabytes (10^u18^ bytes) of information each year--about 250 megabytes for every man, woman, and child on earth. [Lyman, Peter and Hal R. Varian, "How Much Information," 2002, http://www.sims.berkeley.edu/how-much-info] Therefore better tools and technologies for information access and information management are needed to take full advantage of ever-increasing amounts of digital information. The discussion here will focus on technologies for accessing unstructured, digital multimedia and other complex information, including text, Web pages,

Hersh, W., Over, P.	TREC-2001 Interactive Track Report	Included in NIST SP 500-250, The Tenth Text Retrieval Conference, TREC 2001	4/19/2002

In the TREC 2001 Interactive Track six research teams carried out observational studies which increased the realism of the searching by allowing the use of data and search systems/tools publicly accessible via the Internet. To the extent possible, searchers were allowed to choose tasks and systems/tools for accomplishing those tasks. At the same time, the studies for TREC 2001 were designed to maximize the likelihood that groups would find in their observations the germ of a hypothesis they could test for TREC 2002. This suggested that there be restrictions – some across all sites, some only within a given site – to make it more likely that patterns would emerge. The restrictions were formalized in two sorts of guidelines: one set for all sites

Hogan, M.D.	Challenges in IT Standards	NIST SP 974, Proceedings of the NIST Centennial Symposium: Standards in the Global Economy, Past, Present, and Future	

This article summarizes a talk given at the NIST Centennial Symposium in March 2001.

Huang, P.H., Kacker, R.N.	Repeatability and Reproducibility Uncertainty in Measurement of Trace Moisture Generated Using Permeation Tubes	Metrologia	

Permeation-tube moisture generators are commonly used in industry as calibrated sources of water vapor and carrier gas mixtures. This paper describes repeatability and reproducibility uncertainties obtained with these generators in the range 10nL/L to 100 nL/L. Measurements were performed using three permeation-tube moisture generators of the type used in the semiconductor industry. Four pairs of independent repeat measurements for each nominal level and each generator were made. Two independent methods were used to determine the realized concentration of water vapor. In one method, the calculated value was determined using calibrated permeation rate of permeation-tube and flow rate of dry carrier gas of the permeation-tube generator. This is the industrial method for determining moisture concentration. In the second method, the corresponding measured value was determined using the Low Frost-Point Generator at the National Institute of Standards and Technology (NIST) and a quartz-crystal-micro-balance. The characteristic used to quantify repeatability and reproducibility uncertainties is the calculated value minus the measured value. Repeatability uncertainty ranges from 2 nL/L to 8 nL/L approximately. These uncertainties represent the extent of possible variation in industrial generation of water vapor in carrier gases by permeation-tube moisture generators. The documentary ASTM standard E691-99 was used for statistical analysis.

Hunt, F.Y., Kearsley, A.J., Wan,	A Linear Programming Approach to Multiple Sequence Alignment	Applied Mathematics Letter

The problem of multiple sequence alignment is recast as an optimization problem using Markov decision theory. One seeks to minimize the expected or average cost of alignment subject to data-derived constraints. In this setting the problem is equivalent to a linear program which can be solved efficiently using modern interior-point methods.

Iyer, H.K., Wang, C.M., Mathew, T.	A Generalized Confidence Interval for a Consensus Mean with Applications to Interlaboratory Studies	Journal of the American Statistical Association

We consider a one-way random effects model with unequal sample sizes and heterogeneous variances. Using the method of Generalized Confidence Intervals, we develop a new confidence interval procedure for the mean. The procedure is applicable to small samples. Statistical simulation is used to demonstrate that the procedure maintains coverage probabilities close to the

Iyer, H.K., Wang, C.M., Mathew, T.	Models and Confidence Intervals for True Values in Interlaboratory Trials	Journal of the American Statistical Association

We consider the one-way random effects model with unequal sample sizes and heterogeneous variances. Using the method of generalized confidence intervals, we develop a new confidence interval procedure for the mean. Additionally, we investigate two alternative models based on different sets of assumptions regarding between group variability and derive generalized confidence interval procedures for the mean. These procedures are applicable to small samples. Statistical simulation is used to demonstrate that the coverage probabilities of these procedures are close enough to the nominal value so that they are useful in practice. Although the methods are quite general, the procedures are explained with the backdrop of interlaboratory studies.

Jansen, W.A.	Determining Privileges of Mobile Agents	Computer Security Applications Conference

This paper describes a method for controlling the behavior of mobile agent-system entities through the allocation of privileges. Privileges refer to policy rules that govern the access and use of computational resources and services by mobile agents. Our method is based on extending the platform processing environment, using the capabilities present in most mobile agent systems, and applying two forms of privilege management certificates: attribute certificates and policy certificates. Privilege management certificates are digitally signed objects that allow various policy-setting principals to govern the activities of mobile agents through selective privilege assignment. The 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. The paper also describes applying the scheme to Java-based agent systems.

Jansen, W.A.	A Privilege Management Scheme for Mobile Agent Systems	Electronic Notes in Theoretical Computer Science

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

Jansen, W.A., Karygiannis, T., Gavrila, S., Korolev, V.	Assigning and Enforcing Security Policies on Handheld Devices	Canadian Information Technology Security Symposium

The proliferation of mobile handheld devices, such as Personal Digital Assistants (PDAs) and tablet computers, within the workplace is expanding rapidly. While providing productivity benefits, the ability of these devices to store and transmit corporate information through both wired and wireless networks poses potential risks to an organization's security. This paper describes an approach to assigning and enforcing an organization's security policy on handheld devices. The approach relies on the device holding a valid policy certificate, obtained through synchronization with a user's desktop computer, organizational server, or other means, before conducting any security-sensitive operations. The paper describes a proof-of-concept implementation of the policy certificate issuing tool, policy specification language, certificate representation, and enforcement mechanisms that were used to demonstrate this approach, and discusses the associated benefits and drawbacks.

Jones, A.T., Reeker, L.H., Deshmukh, A.V.	Information: A Key to Supply Chain Performance	ISOMA-International Symposium on Manufacturing and Applications

This paper makes several critical points related to the intrinsic nature of the relationship between information and performance in supply chains. It highlights the co-dependence of information and supply-chain management decisions, stresses the impact of this co-dependence on supply-chain performance, and raises research issues that are fundamental to a better understanding of

Jones, A.T., Reeker, L.H., Deshmukh, A.V.	On Information and Performance of Complex Manufacturing Systems	Manufacturing Complexity Network Conference

This paper makes several critical points related to the intrinsic relationship between information and performance in complex, dynamic systems. Using a manufacturing enterprise as an example, we highlight the co-dependence of information and decision outcomes in such systems, stress the impact of this co-dependence on the evolution and performance of these systems, and raise the research issues that are fundamental to a better understanding of both. We claim that the availability of the right information at the right time is crucial for making good decisions. We argue further that determining whether available information is indeed the right information is a difficult problem. Determining the difference between two information objects, and moreover, the impact of this difference on the decisions made, need to be investigated. Finally, we discuss the dependence of the value of an information object and the decision being made using that object.

Kacker, R.	Combining Information from Independent Similar Studies Using	Journal of Quality Technology

We compare leading statistical methods to combine information from independent similar studies using random effects model. One of the oldest methods is that of Cochran(1954). The method of Paule and Mandel(1982) was developed to determine the consensus value of a measurand from interlaboratory studies. The methods of DerSimonian and Laird(1986) was developed to combine information from clinical trials. Rukhin et al (2000) show that the Paule and Mandel estimate is optimal in the sense of being the restricted maximum likelihood estimate under normality. We show that normality is not needed. The method of Paule and Mandel is universally optimal in generalized (weighted) least-squares theory. We show that all three methods are special cases one theorem. The method of Paule and Mandel is iterative. One reason for the popularity of the method of DerSimonian and Laird is that it is non-iterative. The common theorem that links the three methods suggests a second non-interative method. We include it in the pool for comparison. We compare the methods of Cochran, DerSimonian and Laird, and the second non-iterative method proposed here against the optimal method of Paule and Mandel using six data sets from interlaboratory evaluations. We cannot think of a good reason for not using the optimal methods of Paule and Mandel to combine information from independent similar studies using random effects model. However, if one must use a non-iterative method, the second non-iterative method proposed here approximates the optimal method of Paule and Mandel better than the method of DerSimonian and Laird.

Kacker, R.N., Datla, R., Parr, A.	Combined Result and Uncertainty from Interlaboratory Evaluations Based on the ISO Guide	Metrologia

We address the problem of determining the combined result and the associated uncertainty in measurement of a common measurand by a set of competent laboratories. The issues include the following. What is the combined result and what uncertainty is associated with it? What to do when the expanded uncertainty interval associated with the combined result excludes a non-negligible fraction of the individual laboratory results that are believed to be plausible values of the measurand. We discuss these issues and propose a three-step approach based on the ISO Guide to determine the combined result and the associated standard uncertainty so no result believed, based on scientific judgment, to be plausible is put outside the expanded uncertainty interval. We will illustrate the proposed approach through an application to the recent results of the international comparison of cryogenic radiometers organized by the Consultative Committee for Photometry and Radiometry (CCPR).

Karygiannis, T., Jansen, W.A., Gavrila, S., Korolev, V.	A PDA Security Policy Enforcement	Annual Computer Security Applications Conference

This paper describes a proof-of-concept implementation of a Personal Digital Assistant (PDA) Security Policy Enforcement Tool developed by NIST. This tool can assist enterprise security administrators in setting, updating, monitoring, and enforcing group and individual PDA security policies. The PDA Security Policy Enforcement Tool helps PDA users automatically comply with their organization’s latest security policy.

Kearsley, A.J., Reiff, A.M.	Existence of Weak Solutions to a Class of Nonstrictly Hyperbolic	Pacific Journal of Mathematics

	Conservation Laws with Non-Interacting		

Many applied problems resulting in hyperbolic conservation laws are nonstrictly hyperbolic. As of yet, there is no comprehensive theory to describe the solutions of these systems. In this paper, a proof of existence is given for a class of nonstrictly hyperbolic conservation laws using a proof technique first applied by Glimm to systems of strictly hyperbolic conservation laws. We show that Glimm's scheme can be used to construct a subsequence converging to a weak solution. This paper necessarily departs from previous work in showing the existence of a convergent subsequence. A novel functional, shown to be equivalent to the total variation norm, is defined according to wave interactions. These interactions can be bounded without any

Kelso, J., Arsenault, L.E., Satterfield, S.G., Ketcham, P., Kriz,	DIVERSE: A Framework for Building Extensible and Reconfigurable Device Independent Virtual Environments and Distributed, Asynchronous Simulations	Proceedings of Virtual Reality 2002 Conference, Orlando, Florida, March 24-27, 2002, pp.183-190	3/24/2002

We present DIVERSE, a highly modular collection of complimentary software packages designed to facilitate the creation of device independent virtual environments and distributed asynchronous simulations. DIVERSE is free/open source software, containing both end-user programs and C++ APIs (Application Programming Interfaces). DPF is the DIVERSE graphics interface to OpenGL Performer. A program using DPF can run without modification on platforms ranging from fully immersive systems such as CAVEs to generic desktop workstations. DTK is the DIVERSE toolkit, and contains all the non-graphical components of DIVERSE such as networking utilities, hardware device access and navigational techniques. We will describe the design of DIVERSE and present a specific example of how it is being used to aid researchers.

Koichiro, B., Gharavi, H.	IEEE 802.11 FHSS Receiver Design for Cluster-based Multihop Video Communications	NISTIR and Journal of Wireless Communications and Mobile Computing	

Recently, we proposed an ad-hoc, cluster-based, multihop network architecture for video communications using IEEE 802.11 FHSS (Frequency Hopping Spread Spectrum) wireless LAN technology with 2GFSK (2-level Gaussian Frequency Shift Keying) modulation capable of 1 Mb/s transmission. To increase the transmission rate to 2 Mb/s for higher quality video communications, we evaluated the performance of the IEEE 802.11 FHSS system when a 4GFSK modulation option is selected. Since the 2 Mb/s system utilizing 4GFSK modulation is not very efficient in terms of RF range, to improve its performance for multihop applications a combination of diversity and non-coherent Viterbi equalizer are considered. For video transmission, we employed a bitstream splitting technique together with a packet-based error protection strategy to combat packet drops under multipath fading conditions. The real-time transport protocol (RTP), user datagram (UDP), and Internet protocol (IP) are used for video streaming. This includes an RTP packetization scheme to control the packet size and to improve the error resilient decoding of the partitioned video signal. The paper includes the simulation results showing the effects of the receiver design and diversity on

Kuhn, D.R., Frankel, S.E., Tracy,	Security for Telecommuting and Broadband Communications	NIST SP 800-46 (http://csrc.nist.gov/publications/nistpubs/index.html)	9/3/2002

This document introduces broadband communication technologies, and the security considerations associated with them. It discusses the use of a personal firewall, which is essential in protecting a home computer from intrusion; provides instructions on how to configure PCs and web browsers for added security. It also explains home networking, and how a home network can be protected; and describes virtual private networks, which are sophisticated technologies that can provide telecommuters with security approximating that available from an isolated inter-office network. This publication compares alternative approaches for securing e-mail and data transfer, depending on the user’s needs and value of the data., and summarizes considerations for telecommuting security. Appendixes provide useful checklists, software update procedures, and pointers to additional resources

Kuhn, D.R., Reilly, M.J.	An Investigation of the Applicability of Design of Experiments to Software	27th NASA/IEEE Software Engineering Workshop, Greenbelt, Maryland, December 4-6, 2002	

Methods from the field of design of experiments (DOE) have been applied to quality control problems in many engineering fields for several decades. DOE seeks to maximize the amount of information gained in an experiment by optimizing the combinations of independent variables. Software testing using DOE methods, often referred to as combinatorial testing methods, have been advocated as an efficient means of providing a high level of coverage of the input domain with a small number of tests [McGregor, Sykes, 2001; Pressman, 2001]. Algorithms based on orthogonal arrays are available that can generate test data for all 2-way (or higher order n-way) combinations at a reasonable cost. Some authors have proposed the reasonable hypothesis that a point of diminishing returns is reached for some small value of n, so that an effective test strategy is to test n-way combinations of parameter values, with additional tests for selected higher order combinations. Some important questions in this regard are: 1.Is there in fact such a point of diminishing returns? 2.What is the appropriate value of n for particular classes of software? 3.Does this value differ for different types of software, and by how much? In this paper we report on work that begins to answer these questions by characterizing faults in two large open source software projects by the number of conditions required to trigger the fault.

Laskowski, S.J., Morse, E.L.	The Common Industry Format (CIF) is	Usability Professionals Association	

	Now an ANSI/INCITS Standard	

The IUSR (Industry USability Reporting) project, led by NIST (National Institute of Standards and Technology), is developing approaches for increasing the visibility of software usability. Participants are from prominent software supplier and customer organizations. This poster presents an overview of the IUSR project and its major deliverable, the Common Industry Format (CIF), for reporting the results of usability tests.

Laskowski, S.J.; Landay, J.A.; Lister, M.	Automatic Capture, Representation, and Analysis of User Behavior	Conference on Human Factors in Computing Systems, CHI 2002

With the advent of the Web and the refinement of instrumentation and monitoring tools, software user interactions are being captured on a much larger scale than ever before. Automated support for the capture, representation, and empirical analysis of user behavior is leading to new ways to evaluate usability and validate theories of human-computer interaction. It enables remote testing, allows testing with larger numbers of subjects, and motivates the development of tools for in-depth analysis. The data capture can take place in a formal experimental setting or on a deployed system. The main questions are: can we leverage these capabilities to validate or change our models, to improve the user experience, and to change the user interfaces in products in measurably better ways? How will human-computer interaction (HCI) and usability engineering (UE) as bodies of knowledge and practice change? How has HCI/UE research and practice changed as new analysis, design, and evaluation methods have emerged and been adopted? Specifically, a number of different approaches based on these methods have appeared in the research literature [3,7] and in commercial tools [1,5,6,9]. However, these have led to a number of unresolved issues under discussion in both the HCI and UE communities, such as how and when to apply these methods, when is remote, automated testing useful, and what can server logs provide.

Lee, K.H., Choy, Y.C., Cho, S.B., Tang, X., McCrary, V.R.	Change Detection between XML Documents	Lecture Notes in Computer Science (Proceedings of International Workshop on XML-Based Data Management)

This paper presents an efficient algorithm to detect changes between old and new versions of an XML document. The difference between the two versions can be considered to be an edit script that transforms one document tree into another. The proposed algorithm is based on a hybridization of bottom-up and top-down methods: the matching relationships between nodes in the two versions are produced in a bottom-up manner and then the top-down breadth-first search computes an edit script. Faster matching can be achieved because the algorithm does not need to investigate possible existence of matchings for all nodes.

Furthermore, it can detect structurally meaningful changes such as the movement and copy of a subtree as well as simple

Lee, K.H., Choy, Y.C., Cho, S.B., Tang, X., McCrary, V.R.	Content Migration: From Paper to XML Documents	Lecture Notes in Computer Science (Proceedings of International Workshop on Multimedia Data and Document Engineering)	

With the widespread of XML documents on the Web, there is a growing interest in transforming paper-based documents into XML representations. In this paper, we present a syntactic method for logical structure analysis of documents with multiple pages and hierarchical structure. To generate a logical structure more accurately and quickly than previous works of which the basic units are text lines, the proposed method takes text regions with hierarchical structure as input. Furthermore, we define a document model that is able to represent explicit knowledge about geometric characteristics and logical structure information of documents efficiently. Experimental results with 372 images scanned from technical journal documents show that the method has performed logical structure analysis successfully. Particularly, the method generates XML documents as the result of structural analysis, so that it enhances the reusability of documents.

Lee, K.H., Slattery, O.T., Lu, R., Tang, X., McCrary, V.R.	The State of the Art and Practice in Digital Preservation	NIST Journal of Research, Vol. 107, No. 1, pp. 93-106, January-February 2002	2/1/2002

The goal of digital preservation is to ensure long-term access to digitally stored information. In this paper, we try to present a comprehensive survey of techniques used in digital preservation. We also introduce representative digital preservation projects and case studies for better insight into the advantages and disadvantages of different preservation strategies. Finally, the pros and cons of current strategies, critical issues for digital preservation, and future directions are discussed.

Lee, S., Griffith, D.W., Song, N-O.,	A New Analytical Model of Shared Backup Path Provisioning in GMPLS	Photonic Networks Communications, March/April 2002	

As GMPLS and its supporting set of protocols develop into a viable control plane for optical networks, an important function that they will need to support will be the protection and restoration function that has been a major feature of legacy optical networks. A network with a robust set of protection and restoration mechanisms will be able to support data traffic while allowing faster recovery from failures than can be obtained using layer 3 rerouting. Several models have been proposed for protection with GMPLS using shared backup paths. This previous work has not investigated the effect on recovery time critical to the service or the number of backup paths that are required to meet a desired level of performance. Using both restoration time and recovery blocking probability, we have developed a new analytic model for GMPLS-based recovery in M : N protection groups. Furthermore, we show that smaller backup paths can be reserved by capturing the effect of multiple failures in the case of M : N shared protection with revertive mode in an optical network with a GMPLS control plane.

Leigh, S., Heckert, A., Rukhin, A. L., Phillips, J, Grother, P., Newton, E.; Moody, M.; Kniskern, K.; Heath,	Transformation, Ranking, and Clustering for Face Recognition Algorithm Comparison	Third Workshop on Automatic Identification Advanced Technologies, Tarrytown, New York, March 14-15, 2002	

The performance of face recognition algorithms is recently of increased interest, although to date empirical analyses of algorithms have been limited to rank-based scores such a cumulative match score and receiver operating characteristic. This paper demonstrates that algorithms that report ratio scale similarities between unknown and gallery images can be normalized so that a large body of classical statistical methods can be applied to measure recognition performance.

Lennon, E.B., Editor	Contingency Planning Guide for Information Technology Systems	ITL Bulletin, June 2002	6/12/2002

This ITL Bulletin summarizes NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.It describes the process of developing contingency plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.

Lennon, E.B., Helfer, M.	2001 ITL Technical Accomplishments	NISTIR 6815	12/12/2001

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY2001. Following the Director's Foreword and the ITL overview, technical projects in ITL focus areas are described, followed by services to NIST, Industry and international interactions, and staff recognition.

Liggett, W.S.	Nonparametric and Semiparametric Models in Comparison of Observations of a Particle-Size Distribution	Journal of the Japanese Society of Computational Statistics

Testing hypotheses about pairs of unnormalized histograms motivates this paper. The histograms contain particle counts for particle-size intervals. The analysis involves generalized-linear-model fitting of cubic splines with irregularly-spaced knots. Of interest is testing the null hypothesis that two sets of particle counts correspond to intensity functions that differ only by a scale factor and a constant shift in horizontal registration. An unknown smooth function is common to the two intensities. The alternative hypothesis is that in addition, the difference between the two intensities is also an unknown smooth function. We consider three approaches to knot placement. First is specification of so many knots that adequate representations of the unknown functions cannot be doubted. Second is data-driven choice of knots. Third is choice of knots based on prior knowledge of what intensity differences are plausible. For the data at hand, we show that specification of too many knots leads to tests with too little power and that data-driven knot selection can lead to false rejection of the null hypothesis. The data at hand seem to call for use of prior knowledge to construct a semiparametric model that incorporates the distinction between the

Liggett, W.S., Over, P., Buckley,	Empirical Evaluation of Information Retrieval Systems	Journal of Classification

Consider a large document collection, a group of topics (information needs), a designation of each document in the collection as relevant or not relevant to each topic, and information retrieval systems that respond to a query (a natural language statement of a topic) with an ordered list of 1000 documents from the collection. The goal is to draw conclusions about systems from the relation between the system responses and the relevance designations. Alternative queries for the same topic make possible a new approach to this goal because system responses to a battery of queries provide insight into the topic properties that influence system behavior. These topic properties, which can be regarded as latent variables, arise from the possibilities for natural language expression that the queries exhibit. An example of such a property is the extent to which a single key word or phrase distinguishes relevant documents from the others. Summarizing such insights over a group of topics using a form of archetypal analysis leads to general conclusions about system behavior. To illustrate our approach, we use system responses from NIST's Text Retrieval Conference (TREC) to compare two systems with different forms of query processing.

Liu, H.K., Zhang, N.F.	Bayesian Approach to Combining Results From Multiple Methods	Proceedings of the American Statistical Association

Many solutions to the problem of estimating the consensus mean from the results of multiple methods or laboratories have been proposed. In a Bayesian analysis, the consensus mean is specified through probabilistic dependency as either a “parent” or a “child” of the method means. In this paper, we propose a unified approach to some of these Bayes solutions by expressing the consensus mean as a measurable function of the method means and some ancillary variable. This measurement Equation Approach is the standard approach used the ISO Guide to the Expression of Uncertainty in Measurement (ISO GUM). When the measurement equation is linear in the ancillary variable, the uncertainty of our Bayes estimator has a decomposition that is ISO

Lozier, D.W.	The DLMF Project: A New Initiative in Classical Special Functions	Proceedings of International Workshop on Special Functions, Hong Kong. World Scientific Publishing Co., Inc., London WC 2H 9HE, England, June 21 – 25,

NIST (formerly, National Bureau of Standards) has started an ambitious project that aims to produce a successor to Abramowitz and Stegun's {\em Handbook of Mathematical Functions}, published by the National Bureau of Standards in 1964 and reprinted by Dover in 1965. Both editions continue to sell briskly and are widely cited in the scientific literature. However, with the many advances in the theory, computation and application of special functions that have occurred since 1960, a new standard reference is badly needed. NIST intends to satisfy this need by providing a Digital Library of Mathematical Functions (DLMF) as a free Web site together with an associated book and CD-ROM. The Web site will provide many capabilities that are impossible

Lyle, J.R.	NIST CFTT: Testing Disk Imaging Tools	Digital Forensic Research Workshop, August 7-9, 2002, Syracuse University, Syracuse N.Y., International Journal of Digital Evidence, (on line at www.ijde.org)

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A capability is required to ensure that forensic software tools consistently produce accurate and objective test results. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. A methodology consisting of tool requirements specifications, test procedures, test criteria, test sets, and test hardware was developed.This paper reports on the initial CFTT work at NIST as applied to disk imaging tools. A brief overview of the testing process developed at NIST is presented followed by a discussion of the lessons learned testing the developed methodology on two disk imaging tools, dd and SafeBack.

Lyle, J.R.	FS-TST: Forensic Software Testing Support Tools Requirements, Design Notes and User Manual	web (http://www.cftt.nist.gov/)	4/24/2002

This document describes FS-TST Release 1.0. A software package developed to aid the testing of disk imaging tools typically used in forensic investigations. The package includes programs that use the interrupt 13h BIOS disk interface to initialize disk drives, detect changes in disk content, compare pairs of disks, and simulate bad sectors on a disk. Most of the software is written in Borland C++ 4.5 with a few parts written in Borland Assembler. The software can be used in the DOS 6.3 environment to setup disk drives for tests, measure the results of a test and aid in documenting test runs. The intended audience for this document should be familiar with the DOS operating system, computer operation, computer hardware components such as hard drives, hard drive interfaces (e.g., IDE or SCSI) and computer forensics. A working knowledge of C and Assembly programming is not necessary for understanding but would be helpful. The package can be obtained from the WWW at the

Lyle, J.R.	Setup and Test Procedures dd (GNU fileutils) 4.0.36 Forensic Tests	web (http://www.cftt.nist.gov/)	7/10/2002

This document describes the testing of dd (GNU fileutils) 4.0.36 as a disk imaging tool on a Linux platform. The Linux version used was Linux version 2.4.2-2 (Red Hat Linux 7.1 2.96-79). The test cases that were applied are described in Disk Imaging Tool Specification, Version 3.1.6.The tests were run on five 933 Mhz computers. A variety of hard drives (7 different models, 5 major brands) were used for the tests. The source disks (the ones that are copied from) were setup with FAT16, FAT32, NTFS or Linux EXT2 type partitions to represent the most common partition types.The main objective of this document is to provide enough information about the testing process for either an independent evaluation of the process or independent replication of the results. The intended audience for this document should be familiar with the DOS operating system, Linux (or some UNIX like) operating system, computer operation, computer hardware components such as hard drives, hard drive interfaces (e.g., IDE or SCSI) and computer forensics.The document can be obtained from the WWW at the HTTP://WWW.CFTT.NIST.GOV web site.

Marbukh, V.	QoS Routing Under Adversarial Binary Uncertainty	Proceedings of International Conference on Communications (ICC 2002), New York, New York, April 2002

A cost based admission control and routing scheme admits an arriving request on the minimum cost route if this cost does not exceed the cost of the request, and rejects the request otherwise. Cost based strategies naturally arise as a result of optimization of the network performance or incorporating Quality of Service (QoS) requirements into the admission and routing processes. In the former case the implied cost of the resources represents expected future revenue losses due to insufficient resources to service future requests. In the latter case the cost of a route represents the expected level of QoS, e.g., bandwidth, delay, packet loss, etc., provided to the request carried on this route. This paper explores different approachs intended to guard against adversarial uncertainty, i.e., worst case scenario, with respect to the resource costs lying within known "confidence" intervals. We assume that the network minimizes and the adversarial environment maximizes the loss or risk resulted from non-optimal admission and routing decisions due to the uncertainty. In a symmetric case we explicitly identify the

Marbukh, V., Su, D.H.	A Framework for Performance Evaluation and Optimization of an Emerging Multimedia DS-CDMA	Proceedings of 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, July 15-21, 2001

This paper proposes a framework for performance evaluation m~d optimization of an emerging multimedia, packet Direct-Sequence Code Division Multiple Access (DS-CDMA) network with a wide range of Quality of Service (QoS) requirements on losses and delays. The need for a new framework arises from inability of the traditional approach, based on the outage probability, to capture the queueing aspects of DS-CDMA network behavior in presence of delay tolerant traffic. Accounting for these aspects becomes essential for emerging multimedia DS-CDMA networks attempting to approach their capacity limits by using coding and spreading gain control, retransmissions, as well as transmission scheduling/power control. Since in a DS-CDMA network transmissions compete for simultaneous access to several resources, including wireless bandwidth and transmission power, the paper proposes to approximate the feasible QoS region for the network by the intersection of the feasible QoS regions for the corresponding single-resource systems. The feasible QoS region for a single-resource system is estimated by using M / G / 1 conservation laws. Based on this "bottleneck resource" approximation, the paper estimates the admission region for the network and outlines the approach to the network management aimed at maximizing the admission region.

Martys, N.S., Hagedorn, J.G.	Multiscaling Modeling of Fluid Transport in Heterogeneous Materials Using	Concrete Science and Engineering

Discrete Boltzmann Methods

The lattice Boltzmann method is a promising approach for modeling single and multicomponent fluid flow in complex geometries like porous materials. Here, we review some of our previous work and discuss some recent developments concerning fluid flow in multiple pore size materials. After presenting some simple test cases to validate the model, results from large scale simulations of single and multi-component fluid flow through digitized Fountaine sandstone, generated by X-Ray microtomography will be given. Reasonably good agreement was found when compared to experimentally determined values of permeability for similar rocks. Finally, modification of the lattice Boltzmann equations, to describe flow in microporous materials is described. The potential for modeling flows in other microstructures of interest to concrete technology will be discussed.

Maximon, L.C.	The Dilogarithm Function for Complex Argument	NIST Journal of Research	

This paper summarizes the basic properties of the Euler dilogarithm function, often referred to as the Spence function. These include integral representations, series expansions, linear and quadratic transformations, functional relations, numerical values for specialarguments, and its relation to the hypergeometric and generalized hypergeometric function. The basic properties of the two functions closely related to the dilogarithm -- the inverse tangent integral and Clausen's integral -- are also included. A brief summary of the definingequations and properties for the frequently utilized generalizations of the dilogarithm (polylogarithm, Nielsen's generalized polylogarithm, Lerch's transcendent) is also given. Critical references to details concerning these functions

McCrary, V., Floyd, M.	Electronic Book 2001 – Authors, Applications, and Accessibility	NISTIR 6817	

This document summarizes the presentations from Ebook 2001, November 5-7, 2001.

McCrary, V., Floyd, M.	DVD 2002: Standards, Applications, Technology Conference & Exhibition	NISTIR 6880	6/3/2002

Proceedings of DVD 2002: Standards, Applications, Technology Conference & Exhibition, including biographies and speeches of the keynote speakers.

McCrary, V.R., Costello, J.H.	DVD '99 Workshop: Standards, Applications, and Technology	NISTIR 6852

Proceedings of DVD ’99 Workshop: Standards, Applications, and Technology including the speeches of the keynote speakers.

McFadden, G.B.	Phase-Field Models of Solidification	Proceedings of the 2001 John H. Barrett Memorial Lectures

Phase-field models of solidification are presented in the context of diffuse-interface theories based on conserved and non-conserved order parameters. Phase-field models for single-component materials are derived, and the sharp-interface limits that relate the models to conventional sharp-interface theories are discussed. Numerical calculations of dendritic growth are presented to illustrate the application of these techniques. Phase-field models for binary alloys are also given, with representative numerical calculations. Extensions to phase transitions with hydrodynamic or elastic effects are also given. The ability of diffuse-interface theories to capture interfacial phenomena such as wetting, adsorption, solute trapping, surface stress,

McFadden, G.B., Coriell, S.R., Moffat, T.P., Josell, D., Wheeler, D., Schwarzacher, W., Mallett, J.	A Mechanism for Brightening: Linear Stability Analysis of the Curvature Enhanced Coverage Model	Journal of the Electrochemical

This work presents experiments and theory describing a mechanism for how brighteners in electrolytes function. The mechanism involves change of local coverage of a deposition rate enhancing catalyst adsorbed on the surface through change of local surface area during growth as well as accumulation and consumption. A first order perturbation analysis shows the surface is stable against growth of perturbations for all wavelengths above a critical value that is deposition condition dependent. The model predictions are shown to be consistent with the experimental results.

McFadden, G.B., Coriell, S.R., Murray, B.T.	Convective and Morphological Instabilities during Crystal Growth	Proceedings of the 2002 NASA Microgravity Materials Science Conference, Hunstville, AL, June 24-26, 2002

During crystal growth or solidification of a binary alloy from a liquid phase, temperature and solute gradients are inherently present and can give rise to fluid flow in the melt. The interaction of fluid flow with the crystal-melt interface plays an important role in determining the properties of the solidified material. Convection in the melt and interface instability may both produce solute inhomogeneities. The coupling between morphological instability and fluid flow can be complicated; interfacial instabilities depend on temperature and solute gradients that may be strongly influenced by the flow field. The flow field, in turn, may be influenced by the morphology of the interface. Examples of the effects of coupling on the stability of the system are

Mell, P., Grance, T.	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme	NIST SP 800-51(http://csrc.nist.gov/publications/nistpubs/index.html)	9/3/2002

The Common Vulnerabilities and Exposures (CVE) vulnerability naming scheme is a dictionary of common names for publicly known information technology (IT) system vulnerabilities. It is an emerging industry standard that has achieved wide acceptance by the security industry and a number of government organizations. Federal departments and agencies should use this standard for computer vulnerability related activities.

Mell, P., Lippman, R., Haines, J., Hu, V., Zissman, M.	An Overview of Issues in Intrusion Detection System Testing	Recent Advances on Intrusion Detection Symposium 2002	

Intrusion detection systems are becoming ubiquitous defenses in today's networks and yet we have no comprehensive or scientifically rigorous methodology to test the effectiveness of these systems. This paper explores the types of performance measurements that are desired and have been used in the past and reviews many pat evaluations designed to assess these metrics. We also discuss hurdles that have blocked successful measurements in this area and present research suggestions

Mell, P., Tracy, M.	Procedures for Handling Security	NIST SP 800-40 (http://csrc.nist.gov/publications/nistpubs/index.html)	9/3/2002

Timely patching is critical to maintain the operational availability, confidentiality, and integrity of IT systems. However, failure to keep operating system and application software patched is the most common mistake made by information technology (IT) professionals. To help address this growing problem, this special publication recommends methods to help organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. This document also covers areas such as prioritizing patches, obtaining patches, testing patches, and applying

Miller, B.R., Youssef, A.	Technical Aspects of the Digital Library of Mathematical Functions	Annals of Mathematics and Artificial Intelligence Kluwer Academic Publishers, The Netherlands

The NIST Digital Library of Mathematical Functions (DLMF) Project, begun in 1997, is preparing a handbook and Web site intended for wide communities of users. The contents are primarily mathematical formulas, graphs, methods of computation, references, and links to software. The task of developing a Web handbook of this nature presents several technical challenges. We describe the goals of the Digital Library of Mathematical Functions Project and the realities that constrain those goals. We propose practical initial solutions, in order to ease the authoring of adaptable content: a LaTeX class which encourages a modestly semantic markup style; and a mathematical search engine that adapts a text search engine to the task.

Mills, K.L., Yuan, J.	Understanding the Correlation Structure of Network Traffic	ACM/IEEE Transactions on Networking

This paper aims to improve current understanding of the correlation structure of traffic carried over large networks, such as the Internet. To achieve this aim we use simulation, adopting a methodology of homogenization to achieve a sufficiently large model with well-understood parameters. Such a model enables systematic study of fundamental causalities arising from interactions among factors in the application layer, the transport layer, and the network structure. Focusing the model on describing comparative rather than absolute behavior, we undertake a systematic search, using wavelet-based analysis, to identify and understand significant phenomena influencing the correlation structure of network traffic. We find significant interaction between offered traffic and network congestion, andwe conclude that the correlation structure of network traffic should be controllable by modulating available resources. We also find thatcongestion-control mechanisms affect the characteristics of timescale dynamics in network traffic. We illustrate how variability in networkstructure leads to changes in correlation structure. In particular, we find a similar correlation structure to that seen for measured Internet traffic may arise in very large networks, even without high user variability. Our findings imply that observed traffic characteristics might be a combined effect of many factors, including user behavior, transport mechanism, and network structure. Our results suggest that while searching for invariants from empirical observations, one must take care to identify combined effects. Finally, results discussed in this paper suggest that network scale has a more general influence on correlation structure than other properties, such as heavy-tailed file

Mitchell, W.F.	The Design of a Parallel Adaptive Multi-level Code in Fortran 90	Proceedings of the 2002 International Conference on

Software for the solution of partial differential equations using adaptive refinement, multi-level solvers and parallel processing is complicated and requires careful design. This paper describes the design of such a code, PHAML. PHAML is written in Fortran 90 and makes extensive use of advanced Fortran 90 features, such as modules, optional arguments and dynamic memory, to provide a clean object-oriented design with a simple user interface.

Morse, E.L.	Evaluation Methodologies for Information Management Systems	D-LIB Magazine

The projects developed under the auspices of the Defense Advanced Research Projects Agency (DARPA) Information Management (IM) program are innovative approaches to tackle the hard problems associated with delivering critical information in a timely fashion to decision makers. To the extent that each of the information management systems interfaces with users, these systems must undergo testing with actual humans. The DARPA IM Evaluation project has developed an evaluation methodology that can assist system developers in assessing the usability and utility of their systems. The key components of an evaluation plan are data, users, tasks and metrics. The evaluation project recruited six IM project Principal Investigators (PI's) and devoted a year's effort in developing a method for getting from exploring and implementing systems to actually planning and performing structured, hypothesis-based evaluations. Five of the projects participated in this effort while a sixth project was integrated into and evaluated with a larger effort. This report describes the component systems, evaluation factors, and our

Morse, E.L.	Rapid, Remote, Automated Card Sorting using WebCAT	Proceedings of the Usability Professionals’ Association, Eleventh Annual Conference, Orlando, Florida, July 8-12, 2002

WebCAT is a rapid, remote, and automated method for performing card sorting. WebCAT, a tool from the NIST Web Metrics

Testbed, provides a web-based interface for performing card sorting. Its three major parts are: interface for experimental design, drag-and-drop sorting applet, and an analysis component with interactive visual and tabular reports.

O'Hern, C.S., Langer, S.A., Liu, A.J., Nagel, S.R.	Random Packings of Frictionless	Submitted to Physical Review

We study random packings of frictionless particles at T=0. The packing fraction where the pressure becomes nonzero is the same as the jamming threshold, where the static shear modulus becomes nonzero. The distribution of threshold packing fractions narrows and its peak approaches random close-packing as the system size increases. For packing fractions within the peak, there is no self-averaging, leading to exponential decay of the interparticle force distribution.

Ono, I.K., O'Hern, C.S., Langer, S.A., Liu, A.J., Nagel, S.R.	Effective Temperatures of a Driven System Near Jamming	Physical Review Letters

Fluctuations in a model of a sheared, zero-temperature foam are studied numerically. Five different quantities that reduce to the true temperature in an equilibrium thermal system are calculated. All five have the same shear-rate dependence, and three have the same value. Near the onset of jamming, the relaxation time is the same function of these three temperatures in the sheared system as of the true temperature in an unsheared system. These results imply that statistical mechanics is useful for the system and provide strong support for the concept of jamming.

Ono, I.K., Tewari, S., Langer, S.A., Liu, A.J.	Velocity Fluctuations in a Steadily Sheared Model Foam	Physical Review E

Numerical simulations are conducted to calculate velocity fluctuations in a simple two-dimensional model of foam under steady shear. The width of the velocity distribution increases sublinearly with the shear rate, indicating that velocity fluctuations are large compared to the average flow at low shear rates (stick-slip flow) and small compared to the average flow at large shear rates. Several quantities reveal a crossover in behavior at a characteristic strain rate, ?x, given by the yield strain divided by the duration of a bubble rearrangement event. For strain rates above ?x, the velocity correlations decay exponentially in space and time and the velocity distribution is Gaussian. For strain rates below ?x, the velocity correlations decay as stretched exponentials in space and time, and the velocity distribution is broader than a Gaussian.

Onyshczak, R.J., Youssef, A.	Fingerprint Image Compression and the Wavelet Scalar Quantization	Chapter of Advances in Automatic Fingerprint Recognition, Springer-Verlag, London, England, Summer 2002

Due to the large number and size of fingerprint images, data compression has to be applied toreduce the storage and communication bandwidth requirements of those images. In responseto this need, the FBI developed a fingerprint compression specification, called Wavelet ScalarQuantization (WSQ). As the name suggests, the specification is based on wavelet compression.In this chapter, we will review the WSQ specification, and discuss its most important theoreticaland practical underpinnings. In particular, we present the way wavelet compression generallyworks, and address the choice of the wavelet, the structure of the subbands, the differentquantization rates of the various subbands, and the entropy coding of the quantized

Podio, F.L.	Personal Authentication Through Biometric Technologies	Proceedings of the 4TH IEEE International Workshop on Network Appliances

Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use. Recent advances in reliability and performance and recent cost drops make these technologies attractive solutions for access to many computers and networks, for the protection of digital content and for secure access to resources such as network appliances and personal network environments. Access control to doors and other enclosures done through a video camera and a face recognition system, access to a security or gun vault after an iris check or access to a computer granted by checking a fingerprint may soon be a reality. Will biometrics play a key role in personal authentication in the home? Do intelligent network appliances need strong personal authentication? That will depend on the value of the asset that is being protected, the consequence of malicious access to the data (e.g., impact of an unauthorized electronic financial transaction), or access to devices by unauthorized individuals. Examples of this need include restricted access to specific TV channels, cable set-top box access, access control to drug cabinets and logical access control to devices that would allow an individual to access financial data, medical records, and other private data. Strong security is encouraged, especially when home appliances can be remotely controlled. Unlike passwords, Personal Identification Numbers or smart cards, biometric characteristics cannot be shared, lost or stolen. How far we are from these scenarios in the world of network appliances? Are biometrics standards in place that would allow for easy biometric data interchange among devices and for interoperability of biometric-based network appliances from different providers? These topics, utilization scenarios in the home and an introduction to the state-of-the art will be discussed.

Podio, F.L., Dunn, J. S., Editors
Proceedings of the Biometric Consortium Conference, September
NISTIR 6911
9/23/2002

The Biometric Consortium Conference examines rapid advances in biometric technologies and applications andexplores new developments in the areas of metrology, assurance, and standards. The Conference proceedings include presentations in a series of topics that address user requirements for Homeland Security and industry response to these requirements, technological issues and challenges looming ahead, other government and commercial implementations and initiatives, biometric business models, updates on the latest activities in measurements and standards, testing, interoperability and data interchange, biometrics security and assurance, and novel applications of biometrics (e.g., Point of Sale, and large-scale enterprise network authentication environments). Seminars included in the Proceedings address overview of biometrics, biometrics market development, biometric template protection and usage, developing BioAPI and CBEFF-compliant biometric authentication

Reeker, L.H., Jones, A.T.
Measuring the Impact of Information on Complex Systems
NIST SP 982, Measuring the Performance and Intelligence of Systems: Proceedings of the 2001 PerMIS Workshop, Mexico City, Mexico, September 4, 2001
6/1/2002

The application of power-driven machinery to manufacturing and other areas of human endeavor characterized the Industrial Revolution in the 18th and 19th centuries. Measurement contributed in many ways to the increasing economic influence of these machines. Using formal or informal physical principles, metrics and measurement techniques were found that allowed the comparison of machine performance (evaluation), the development of machines with the needed qualities (engineering), and the coordination of machines within factories (integration). The required physical dimensions were space, time, and mass, and the common physical quantities derived from these three; and, for these quantities, measurement techniques were established. In the Information Revolution begun in the 20th Century, measuring information is also vital to the continued influence of machines. Unfortunately, information is not as well understood, as are physical constructs. It seems to have an unlimited number of dimensions, and no generally accepted metrics or measurement procedures. So how do we measure the impact of information in the 21st Century? This paper sketches research directions that may help to answer this question and it stresses

Reeker, L.H., Jones, A.T.
A New Classification of Information: A Step on the Road to Interpretability
NIST SP 990, Measuring the Performance and Intelligence of Systems: Proceedings of the 2002 PerMIS Workshop

Complex systems, such as manufacturing supply chains, are often modeled as a collection of interacting components with information flows between them. These components are frequently responsible for making a wide range of decisions that are implemented using an optimization, heuristic, or control technique. The traditional approach to system performance focuses on the performance of these components. The view has been that to improve the system performance one had only to develop better techniques. In this paper, we argue that inadequate attention has been paid to the relationship between information and system performance.Information has played an important role in the manufacturing systems of the past. It will play a dominant role in the Internet-based manufacturing systems of the future. To better design, engineer, implement, and control these systems, we need a fundamental understanding of information and its effects on system dynamics. This paper contends that we need a new characterization of information, a delineation of its salient properties, quantitative metrics for those properties, methods for computing these metrics, and linkages between these metrics and system performance. We focus principally on the first of these, a new characterization of information, and discuss the implications of suggested characterizations for metrics and their measurement, suggesting some approaches for further research.

Ressler, S., Wang, Q.	A Web3D Based CAESAR Viewer	CARS 2002 – H.U. Lemke, M.W. Vannier; K. Inamura, A.G. Farman, K. Doi & J.H.C. Reiber (Editors)ÓCARS/Springer

The CAESAR (Civilian American and European Surface Anthropometry Resource) project completed in 2002 has collected 3D scans of over 5000 subjects. We have created a 3D interface, the NIST CAESAR Viewer (NCV), utilizing the Virtual Reality Modeling Language (VRML) to provide 3D access via the Web. In addition to simply viewing the 3D scans we have augmented the display of the body with interactive anthropometric landmarks and contour line displays. The landmarks and viewpoints associated with the landmarks are automatically placed onto the body as a visual anthropometric glossary. Display of the contours boundaries are adjusted by the user moving sagittal, coronal and transverse cutting planes. This paper describes the

Roberts, J.W.	Triggered Image Capture for High Speed Display Characterization	SPIE Electronic Imaging '02 Conference

Precision display measurements often involve the integration of light measurements over many frames. Newer display technologies with high speed light modulators such as micromirrors are able to make sophisticated use of temporal modulation. This may result in measurement errors, and in situations where temporal modulation produces visible artifacts that affect display usability, but that conventional metrology techniques do not detect. There is a need for further development of new metrology techniques that collect information on the temporal behavior of high speed displays. The emergence of multiple technologies from multiple display manufacturers has created a need for generic, non-brand-specific tools.We are working on such a technique, using the triggered capture of display images with a sub-microsecond imager, with test images and image sequences designed to evoke particular display responses, triggers that can involve keying on features designed into the test images, and subsequent processing of captured images to reconstruct the behavior of the display. In principle, such measures can be calibrated with conventional full-screen measurements so that a determination of pixel sequences can lead to an accurate determination of the effective grayscale and luminance of each pixel. Complications include the finite time required for pixel switching (so that pixel duty cycles can not be computed in unit blocks of time), and the risk that the observation method used will introduce a bias in the temporal observations.

Roberts, J.W.	Small-Scale Tactile Graphics for Virtual Reality Systems	SPIE Electronic Imaging '02 Conference

As virtual reality technology moves forward, there is a need to provide the user with options for greater realism for closer engagement to the human senses. Haptic systems use force feedback to create a large-scale sensation of physical interaction in a virtual environment. Further refinement can be created by using tactile graphics to reproduce a detailed sense of touch. For example, a haptic system might create the sensation of the weight of a virtual orange that the user picks up, and the sensation of pressure on the fingers as the user squeezes the orange. A tactile graphic system could create the texture of the orange on the user’s fingertips. In the real world, a detailed sense of touch plays a large part in picking up and manipulating small objects.Our team is working to develop technology that can drive a high density fingertip array of tactile stimulators at a rapid refresh rate, sufficient to produce a realistic sense of touch. To meet the project criteria, the mechanism must be much lower cost than existing technologies, and must be sufficiently lightweight and compact to permit portable use and to enable installation of the stimulator array in the fingertip of a tactile glove. The primary intended applications for this technology are

Roberts, J.W., McCrary, V.R.,	The NIST Rotating Braille Reader for Electronic Books	Included in NISTIR 6817, Proceedings of NIST Electronic Book 2001 Conference

We have developed a new technology to reduce the cost of Braille-based information accessibility. Millions of blind and visually impaired people in the US (and far higher numbers worldwide) need some form of non-visual access to information. The widespread use of Braille displays has been limited primarily by cost and reliability issues. The primary cost and reliability factor is the large number of electromechanical actuators. Each 6/8-dot Braille cell requires 6/8 actuators, with hundreds needed for the entire display. Small displays (e.g. 8-character) are available, but require the user to move a finger back and forth, raising issues of convenience and repetitive stress injuries. Our approach uses as few as 3 to 4 actuators for the entire display. Our objective in undertaking this project was to find a new approach to Braille display design that would significantly lower cost and improve reliability, and still provide a worthwhile reading experience approaching that of full-line (80-character) displays. Our target was a factor of ten reduction in display cost.After successful completion and demonstration of a 2nd-generation working prototype, we have been working to extend the Braille reader technology to graphics, enabling the first practical refreshable

Robertson, S., Soboroff, I.	The TREC-2001 Filtering Track Report	Included in NIST SP 500-250, The Tenth Text Retrieval Conference, TREC 2001	4/19/2002

The TREC-10 filtering track measures the ability of systems to build persistent user profiles which successfully separate relevant and non-relevant documents. It consists of three major subtasks: adaptive filtering, batch filtering, and routing. In adaptive filtering, the system begins with only a topic statement and a small number of positive examples, and must learn a better profile from on-line feedback. Batch filtering and routing are more traditional machine learning tasks where the system begins with a large sample of evaluated training documents. This report describes the track, presents some evaluation results, and provides a general commentary on lessons learned from this year's track.

Rosenthal, L.S.	W3C Quality Assurance Activity	XML 2001 Conference Proceedings	

In order for web specifications to permit full interoperability and access to all, it is important that the quality of implementation be given as much attention as their development. Moreover, as the complexity of W3C specifications and their interdependencies increases, quality assurance becomes even more important to ensuring their acceptance and deployment in the market. To address these needs, the W3C initiated a new Quality Assurance (QA) Activity (http://www.w3.org/QA/) to address all aspects of the quality of the implementations of W3C specifications as well as the quality of the specifications produced by W3C. This session will introduce the audience to this new W3C Quality Assurance Activity by presenting the goals, scope objectives, and expected deliverables of the activity and providing an overview and status report of the Activity's

Ross, R.S.	The New Homeland Security: Challenges for a Great Nation	Government Computer News	1/21/2002

This article reiterates the importance of homeland security in light of the events of September 11th and the necessity to integrate information technology security into enterprise security. Now, more than ever, the challenges of homeland security require a true partnership between government and industry—from conducting cutting edge research and development in information technology security to developing voluntary information technology security standards, testing programs and best practices for our information systems and networks.

Rukhin, A., Grother, P., Phillips, J., Leigh, S.Newton, E., Heckert, A.	Dependence Characteristics of Face Recognition Algorithms	International Conference on Pattern Recognition (ICPR), 2002

Nonparametric statistics for quantifying dependence between the output rankings of face recognition algorithms are described. Analysis of the archived results of a large face recognition study shows that even the better algorithms exhibit significantly different behaviors. It is found that there is significant dependence in the rankings given by two algorithms to similar {\em and} dissimilar faces but that other samples are ranked independently. A class of functions known as copulas is used; it is shown that the correlations arise from a mixture of two copulas.

Rust, B.W.	Fitting Nature's Basic Functions Part III: Exponentials, Sinusoids and Nonlinear Least Squares	Computing in Science and

This paper explains the Gauss - Newton iteration, and the Levenberg - Marquardt variant of it, for nonlinear least squares calculations. It also explains how to compute statistical diagnostics for the fits and to test hypotheses about them. It illustrates these techniques by fitting simple mathematical models to the time series records of annual fossil fuel CO2 emissions and

Sanders, G.A., Le, A.N., Garofolo,	Effects of Word Error Rate in the DARPA Communicator Data During	International Conference on Spoken Language Processing, 2002

During 2000 and 2001 two large data collections were performed, with paid users doing travel planning using eight Communicator spoken dialogue systems. We analyze the effects of speech recognition accuracy, as measured by Word Error Rate (WER), on other metrics. Analysis shows a linear correlation between WER and task completion metrics, which unexpectedly remained linear even at high levels of WER. The determinants of user satisfaction are more complex, but we present evidence suggesting a somewhat linear correlation between WER and satisfaction for WER less than 35% or 40% in 2001 (stronger correlation in 2000). The size of the effect of increasing WER on task completion is about half as large in 2001 as in 2000, demonstrating improved ability to accomplish tasks despite high WER, and we consider this to be an important accomplishment of the research

Scholtz, J.C.	Evaluation Methods for Human-System Performance of Intelligent Systems	Proceedings of Performance Metrics for Intelligent Systems 2002 Conference (PerMIS)	

The paper discusses different roles in human-robot interaction and the evaluation methods that can be used to assess system performance.

Scholtz, J.C.	Human-Robot Interactions: Creating Synergistic Cyber Forces	Proceedings of Workshop on Multi-Robot Systems	

Human-robot interaction for mobile robots is still in its infancy. As robots increase in capabilities and are able to perform more tasks in an autonomous manner we need to think about the interactions that humans will have with robots and what software architecture and user interface designs can accommodate the human-in -the loop. This paper outlines a theory of human-robot interaction and proposes the interactions and information needed by both humans and robots for the different levels of

Scholtz, J.C.	Living and Working with Ubiquitous Computing	Grace Hopper Conference, Vancouver, Canada, October 9-12, 2002	10/9/2002

Today, much of our information-intensive work is carried out at desktop computer workstations; however, increasingly people work and live on the move. Very soon, scads of small information processing appliances will be carried along from place to place as adjuncts to support our jobs. In this paper, we outline specific facets of two grand challenges that the human-computer interaction (HCI) research community must meet in order for society to reap the benefits of numerous, specialized, information devices. As a first grand challenge, researchers must remove the computer barrier between people and information. As grand challenge two, researchers must find a means to endow cyberspace with a better understanding of the physical and logical world in which people live. We discuss some specific research problems that must be solved to meet these two grand challenges. Where applicable, we also point to some ongoing research that appears to be tackling, at an early stage, some aspects of these

Scholtz, J.C., Arnstein, L., Kim, M., Kindberg,T., Consolvo, S.	User-Centered Evaluations of Ubicomp Applications	Proceedings of Ubicomp 2002 Conference

This paper describes some properties of ubiquitous computing applications that warrant user-centered evaluation and describes a number of approaches carried out in recent studies.

Scholtz, J.C., Morse, E.L.	A New Usability Standard and What It Means to You	ACM SIGCHI Bulletin

The Common Industry Format (CIF) was approved on December 12, 2001 as an ANSII standard (ANSI/NCITS-354-2001). The CIF is a deliverable from the Industry USability Reporting (IUSR) Project begun in 1997, facilitated by the National Institute of Standards and Technology (www.nist.gov/iusr). The IUSR group includes representation from prominent suppliersof software, representatives from large consumer organizations, usability consultants, and academics. The goal was to raise the visibility of software usability so that it could be used as a factor when companies are making procurement decisions. The group decided to concentrate its efforts on developing a common usability reporting format for sharing usability data with consumer organizations and validating the format by pilot trials. The resulting CIF does not specify what needs to be tested but details what should be reported about a summative usability evaluation. This information includes the tasks used in the evaluation, the testing environment including hardware, software, and evaluation protocols, the results of the evaluation, the analysis techniques used in determining the results, and the data collection mechanisms. The CIF is meant to be generated and interpreted by usability professionals. It allows consumers to determine if the usability testing done by the software supplier reflects their target users, tasks, and context. Consumer companies can then use thisinformation to determine how the usability of this product will affect their bottom line. The IUSR group is currently conducting pilot studies in which software suppliers are using the CIF to convey usability information to consumers. Consumer organizations are collecting data to benchmark total cost of ownership of individual software applications and using this data to predict the cost/benefits of acquiring new versions of the software based on the usability metrics. NIST continues to facilitate this effort and will be collecting and distributing the process and metrics that the consumer companies find useful. The IUSR group is considering future expansions to the CIF. Extensions currently under consideration include: reporting of Web usability studies, reporting of hardware usability, communicating usability requirements, and accessibility reporting. Other participants are using the CIF as a reporting format for teaching usability and as

Scholtz, J.C., Morse, E.L.	A Standard Reporting Format for Summative Usability Evalutations	Interactions

Poor usability is an uncontrolled source of overhead, caused by the need for users to correct errors and continually re-learn complex user interfaces. Software that is measurably usable reduces errors, reduces training costs, and reduces maintenance costs, while increasing user productivity and satisfaction. The business case for software usability has been clearly established. Many software vendors subject their products to usability testing during the development cycle, however, when companies or organizations make large purchase decisions for software, they currently have little visibility into the usability of the products they are buying. How can these potential software purchasers use usability as a factor in their decisions? An effort to increase the visibility of software usability was begun in October of 1997 by the U.S. National Institute of Standards and Technology (NIST: http://www.nist.gov) and resulted in the creation of the Industry USability Reporting (IUSR) Project (http://www.nist.gov/iusr). Cooperating in this effort are prominent suppliers of software, representatives from large consumer organizations, usability consultants, and academics. NIST's role is to facilitate and co-ordinate the activities of this group of usability advocates.

Early on the group decided to concentrate its efforts on developing a common usability reporting format for sharing usability data with consumer organizations and validating the format by pilot trials. Through a series of four workshops, the IUSR team developed a document called the Common Industry Format for Usability Test Reports (CIF). Members contributed information about the formats that were being used by their companies' usability groups. They determined which elements were essential to a good report and which things were less important. The structure of the essential elements was developed using a consensus process.

The resulting CIF is meant to be generated by a usability professional at the software supplier company and interpreted by a usability professional at the consumer company. It contains an executive summary for management and more detailed sections containing the description of the product, the objectives of the test, demographic data about the participants, the context in which the product was evaluated, the experimental design of the evaluation, the results produced using the CIF metrics of effectiveness, efficiency, and satisfaction, and the data analysis techniques used. Note that the CIF does NOT specify how a usability test is to be performed; it merely stipulates how the results of a test are to be reported. Informational Annexes (Appendices) include a Glossary of terms and a checklist and template (MS Word) to jump-start CIF preparation.

In May 2001, the CIF was submitted to the National Committee for Information Technology Standards (NCITS: http://www.ncits.org/) as a Proposed Standard. NCITS approved the Proposal in November 2001. ANSI (American National Standards Institute) approval on December 12, 2001 resulted in an American national standard for usability reports. ANSI/NCITS-354-2001 contains a description of how the results of a usability test should be reported so that other usability professionals can determine whether the testing reflects their target user, tasks, and context. Now, for the first time, usability information can be factored into purchase decisions. Armed with this information, usability professionals in consumer companies

Scholtz, J.C., Morse, E.L., Laskowski, S.J., Wishansky, A.,	Quantifying Usability: The Industry Usability Reporting Project	Proceedings of the Human Factors and Ergonomics Conference

The paper describes the Common Industry format (CIF) developed in the Industry Usability Reporting Project (IUSR), which is now an ANSI standard. Four pilot studies conducted to verify the usefulness of the CIF are also described.

Schultheisz, C.R., Flynn, K.M.,	Certification of the Rheological	NIST SP 260-147

Leigh, S.D. Behavior of SRM 2491,

The certification of the rheological properties of Standard Reference Material® (SRM) 2491, a non-Newtonian fluid consisting of polydimethylsiloxane, is described. The viscosity and the first normal stress difference were measured in steady shear at rates between 0.001 s-1 and 6.3 s-1 at 0 °C, 25 °C and 50 °C. The linear viscoelastic storage modulus G' and loss modulus G" were also measured in dynamic oscillatory measurements between 0.1 rad/s and 100 rad/s in the temperature range between 0 °C and 50 °C and master curves calculated using time temperature superposition.

Sims, J.S., George, W.L., Satterfield, S.G., Hung, H.K., Hagedorn, J.G., Ketcham, P.M., Griffin, T.J., Hagstrom, S.A., Franiatte, J.C., Bryant, G.W., Jaskilski, W., Martys, N.S., Bouldin, C.E., Simmons, V., Nicolas, O.P., Warren, J.A., am	Accelerating Scientific Discovery Through Computation and Visualization	NIST Journal of Research, Vol. 107, No. 3, May-June 2002,	6/1/2002

This is the second in a series of articles describing a wide variety of projects at NIST that synergistically combine physical science and information science. It describes, through examples, how the Scientific Applications and Visualization Group (SAVG) at NIST has utilized high performance parallel computing, visualization, and machine learning to accelerate research. The examples include scientific collaborations in the following areas: (1) High Precision Energies for few electron atomic systems, (2) Flows of suspensions, (3) X-ray absorption, (4) Molecular dynamics of fluids, (5) Nanostructures, (6) Dendritic growth in alloys, (7) Screen saver science, (8) genetic programming.

Sims, J.S., Hagstrom, S.A.	High Precision Hy-CI Variational Calculations for the Ground State of Neutral Helium and Heliumlike Ions	International Journal of Quantum Chemistry	

Hylleraas-Configuration Interaction (Hy-CI) method variational calculations with up to 4648 expansion terms are reported for the ground ^{1}S state of neutral helium. Convergence arguments are presented to obtain estimates for the exact nonrelativistic energy of this state. The nonrelativistic energy is calculated to be -2.9037 2437 7034 1195 9829 99 a.u. Comparisons with other calculations and an energy extrapolation give an estimated nonrelativistic energy of -2.9037 2437 7034 1195 9830(2) a.u., which agrees well with the best previous variational energy, -2.9037 2437 7034 1195 9829 955 a.u., of Korobov, obtained using the universal (exponential) variational expansion method with complex exponents. In addition to He, results are also included for

Sims, J.S., Mrtys, N.S.	Simulation of Sheared Suspensions with a Parallel Implementation of QDPD	Computer Physics Communications

A quaternion-based dissipative particle dynamics (QDPD) program was developed to study the flow properties of complex fluids like suspensions, subject to shear. To overcome CPU speeds limiting the size and complexity of the simulations that can be carried out with this program, a parallelization of the program has been done using MPI. The technique, a traditional spatial domain decomposition using a parallel link-cell algorithm, has some fairly novel features arising from the DPD formalism (which forces some tricky bookkeeping to satisfy Newton's third law), the use of ellipsoids spread out across processors, and the requirement of a sheared boundary condition. This last condition, shear, can result in particles being moved to a non-neighboring processor at the end of some time steps. A detailed discussion of our implementation is presented, along with results on an IBM SP2 cluster. A parallel speedup of 24.19 was obtained for a benchmark calculation on 27 processors.

Smeaton, A.F., Over, P., Costello, C., Vries, A. P., Doermann, D., Hauptmann, A., Rorvig, M. E., Smith, J. R., Lide, W.	The TREC 2001 Video Track: Information Retrieval on Digital Video	European Digital Libraries Conference 2002

The development of techniques to support content-based access to archives of digital video information has recently started to receive much attention from the research community. During 2001, the annual TREC activity, which has been benchmarking the performance of information retrieval techniques on a range of media for 10 years, included a “track” or activity which allowed investigation into approaches to support searching through a video library. This paper is not intended to provide a comprehensive picture of the different approaches taken by the TREC2001 video track participants but instead we give an overview of the TREC video search task and a thumbnail sketch of the approaches taken by different groups. The reason for writing this paper is to highlight the message from the TREC video track that there are now a variety of approaches available for searching and browsing through digital video archives, that these approaches do work, are scalable to larger archives and can yield useful retrieval performance for users. This has important implications in making digital libraries of video information

Smeaton, A.F., Over, P., Taban, R.	The TREC-2001 Video Track Report	Included in NIST SP 500-250, The Tenth Text Retrieval Conference, TREC 2001	4/19/2002

New in TREC-2001 was the Video Track, the goal of which was to promote progress in content-based retrieval from digital video open, metrics-based evaluation. The track built on publicly available video provided by the Open Video Project of the University of North Carolina at Chapel Hill, the NIST Digital Video Library, and stock shot video provided for TREC-2001 by the BBC. The track used very nice work on shot boundary evaluation done as part of the ISIS Coordinated Research Project. This paper is an introduction to the track framework – the tasks, data, and measures. For information about results, see the tables

Stoneburner, G., Goguen, A., Feringa, A.	Risk Management Guide for Information Technology Systems	NIST SP 800-30 (http://csrc.nist.gov/publications/nistpubs/index.html)	1/31/2002

Risk Management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Organizations use risk assessment, the first step in the risk management methodology, to determine the extent of the potential threat, vulnerabilities, and the risk associated with an information technology (IT) system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, the second step of risk management, which involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems throughout their system development life cycle (SDLC). The ultimate goal is to help organizations to better manage IT-related mission risks.Organizations may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their site environment in managing IT-related mission risks. In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. The third step in the process is continual evaluation and assessment. In most organizations, IT systems will continually be expanded and updated, their components changed, and their software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

Swanson, M., Fabius, J., Stevens, M., McLarnon, M.	Automated Security Self-Evaluation Tool User Manual	NISTIR 6885 (http://csrc.nist.gov/asset/)	11/1/2002

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. This manual is intended to help users of ASSET understand each function of the tool and how the tool can be used to complete self-assessments. The target audience of this manual is the

Swanson, M., Stevens, M., McLarnon, M., Thomas, J.	Automated Security Self-Evaluation Tool (ASSET)	web (http://csrc.nist.gov/asset/)	9/12/2002

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

Swanson, M., Wohl, A., Grance, T., Hash, J.,Pope, L., Thomas, R.	Contingency Planning Guide for Information Technology Systems	NIST SP 800-34 (http://csrc.nist.gov/publications/nistpubs/index.html)	6/11/2002

The Contingency Planning Guide for Information Technology (IT) Systems provides instructions, recommendations, and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services after an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods. The information presented in this document addresses specific contingency planning recommendations and provides strategies and techniques common to desktops and portable systems, servers, Web sites, local area networks, wide area networks, distributed systems, and mainframe systems.The document also defines the following seven-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for their IT systems. These seven progressive steps are to develop the contingency planning policy statement, conduct the business impact analysis (BIA), identify preventive controls, develop recovery strategies, develop an IT contingency plan, plan testing/training/exercises, and plan maintenance are designed to be integrated into each stage of the system development life cycle.

Tanoglu, G.B., Braun, R.J., Cahn, J.W., McFadden, G.B.	A1-L10 Phase Boundaries and Anisotropy via Multiple-Order-Parameter Theory for an FCC Alloy	Submitted to Acta Materialia	

The dependence of thermodynamic properties of planar interphase boundaries (IPBs) and antiphase boundaries (APBs) in a binary alloy on an FCC lattice is studied as a function of the orientation of their normal with respect to the underlying lattice. Using a recently-developed diffuse interface model based on three non-conserved order parameters and the concentration, and an improved free energy density that gives a realistic phase diagram with one disordered phase and two ordered phases such as those that occur in the Cu-Au system, we are able to find IPBs and APBs between any pair of domains and phases, and for all orientations. The model includes bulk and gradient terms in a free energy functional, and assumes that there is no mismatch in the lattice parameters for the disordered and ordered phases so that elastic effects can be neglected. The bulk energy model is based on the multi-atom interaction among at least four neighbors, and the entropy term is taken as due to ideal mixing on each sublattice. In this paper, we set up the governing equation and give a catalog which constitutes the sets of boundary conditions for all IPBs and APBs. We then focus on one specific set as an example, the IPB between the disordered A1 phase and the L10 ordered phase, which could not be calculated with the free energy used previously. For this IPB we compute the numerical solution of the boundary value problem to find its interface profile, its interfacial energy as a function of orientation, temperature, and chemical potential (or composition).

Tracy, M., Jansen, W.A., Bisker,	Guidelines on Electronic Mail Security	NIST SP 800-45 (http://csrc.nist.gov/publications/nistpubs/index.html)	10/3/2002

Electronic mail (email) is perhaps the most popularly used system for exchanging information over the Internet. After Web servers, mail servers are often the most targeted and attacked hosts on an organization's network. Various types of mail content and attachments have also proven to be effective in introducing malicious code into a system through the email client. Thus, it is essential to secure mail servers and clients as well as the network infrastructure that supports them. This document has been developed to assist federal departments and agencies, state agencies, and commercial organizations in installing, configuring, and maintaining secure mail servers and mail clients . It presents generic security principles and covers details specific to the various components of a mail system. It also includes examples that address two of the more popular mail server applications running respectively on Unix and Microsoft Windows operating systems: sendmail and Exchange.

Tracy, M., Jansen, W.A.,	Guidelines on Securing Public Web	NIST SP 800-44	10/3/2002

McLarnon, M.	Servers	(http://csrc.nist.gov/publications/nistpubs/index.html)	

Web servers maintained for public use are normally the most targeted and attacked hosts on an organization’s network. Thus, it is essential to secure Web servers and the network infrastructure that supports them. This document has been developed to assist federal departments and agencies, state agencies, and commercial organizations in installing, configuring, and maintaining secure public Web servers. It presents generic security principles and covers details specific to the various components of Web content, Web applications, and Web servers. It also includes examples that address two of the more popular Web server applications running respectively on Unix and Microsoft Windows operating systems: Apache and Internet Information Server.

Van Dyck, R.E., Doherty, J.F., Wang, Y.	A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images	IEEE Transactions on Image Processing, February/March 2002	3/1/2002

In recent years, access to multimedia data has become much easier due to the rapid growth of the Internet. While this is usually considered an improvement of everyday life, it also makes unauthorized copying and distributing of multimedia data much easier, therefore presenting a challenge in the field of copyright protection. Digital watermarking, which is inserting copyright information into the data, has been proposed to solve the problem. In this paper, we first discuss the features that a practical digital watermarking system for ownership verification requires. Besides perceptual invisibility and robustness, we claim that the private control of the watermark is also very important. Second, we present a novel wavelet-based watermarking algorithm. Experimental results and analyses are then given to demonstrate that the proposed algorithm is effective and can be used in a

Van Dyck, R.E., Kim, T., Miller,	Hybrid Fractal Zerotree Wavelet Image Coding	Signal Processing: Image Communication, 2002	

In this paper, a hybrid fractal zerotree wavelet (FZW) image coding algorithm is proposed. The algorithm couples a zerotree-based encoder, such as the embedded zerotree wavelet (EZW) coder or set partitioning in hierarchical trees, and a fractal image coder; this coupling is done in the wavelet domain. Based on perceptually-weighted distortion rate calculations, a fractal method is adaptively applied to the parts of an image that can be encoded more efficiently relative to an EZW coder at a given rate. In addition to improving compression performance, the proposed algorithm also allows one to impose desirable properties from each type of image coder, such as progressive transmission, the zerotree structure, and range-domain block

Van Dyck, R.E., Soltarian, A.	Performance of the Bluetooth System in Fading Dispersive Channels and Interference	IEEE Globecom 2001, San Antonio, Texas, November 25-29, 2001	11/25/2001

A noncoherent limiter-discriminator receiver is often considered for the Bluetooth system because of its simplicity and low cost. While its performance is more than adequate for some channels, the results are significantly degraded in either an interference-limited environment or a frequency selective channel. In this paper, we compare the performance of the traditional limiter-discriminator with integrate and dump filter to a more sophisticated Viterbi receiver. We find that the Bluetooth access code is sufficient to be used for channel estimation in the Viterbi receiver. A comparison is carried out in a Rayleigh fading channel and in the presence of interference either from another Bluetooth piconet or an IEEE 802.11b wireless local area

Voorhees, E.M.	Overview of the TREC 2001 Question Answering Track	Included in NIST SP 500-250, The Tenth Text Retrieval Conference, TREC 2001	4/19/2002

The TREC question answering track is an effort to bring the benefits of large-scale evaluation to bear on the question answering problem. In its third year, the track continued to focus on retrieving small snippets of text that contain an answer to a question. However, several new conditions were added to increase the realism, and the difficulty, of the task. In the main task, questions were no longer guaranteed to have an answer in the collection; systems returned a response of `NIL' to indicate their belief that no answer was present. In the new list task, systems assembled a set of instances as the response for a question, requiring the ability to distinguish among instances found in multiple documents. Another new task, the context task, required

Voorhees, E.M.	The Philosophy of Information Retrieval Evaluation	Proceedings of the 2001 Cross-Language Evaluation Forum (CLEF) and Springer's Lecture	

Evaluation conferences such as TREC, CLEF, and NTCIR are modern examples of the Cranfield evaluation paradigm. In the Cranfield paradigm, researchers perform experiments on test collections to compare the relative effectiveness of different retrieval approaches. The test collections allow the researchers to control the effects of different system parameters, increasing the power and decreasing the cost of retrieval experiments as compared to user-based evaluations. This paper reviews the fundamental assumptions and appropriate uses of the Cranfield paradigm, especially as they apply in the context of

Voorhees, E.M., Buckley, C.	The Effect of Topic Set Size on Retrieval Experiment Error	SIGIR Conference	

Retrieval mechanisms are frequently compared by computing the respective average scores for some effectiveness metric across a common set of information needs or topics. Since retrieval system behavior is known to be highly variableacross topics, good experimental design requires that a "sufficient" number of topics be used in the test. This paper uses TREC results to empirically derive error rates based on the number of topics used in a test and the observed difference in the average scores. The error rates quantify the likelihood that a different set of topics of the same size would lead to a different conclusion. We directly compute error rates for topic sets up to size 25, and extrapolate those rates for larger topic set sizes.The error rates found are larger than anticipated, indicating researchers need to take care when concluding one method

Voorhees, E.M., Harman, D.	The Tenth Text Retrieval Conference, TREC- 2001	NIST SP 500-250	4/19/2002

TREC 2001 is the latest in a series of workshops designed to foster research in information retrieval and related tasks. This year's conference consisted of six different tasks, including a new task on content-based retrieval of digital video. The overview describes the tenth Text Retrieval Conference held in Gaithersburg, Maryland, November 13-16, 2001. Included are the basics of how TREC is organized, summaries of the main results of each of the TREC 2001 tasks, and reports on initial plans for TREC

Wack, J.	Guidelines on Firewalls and Firewall	ITL Bulletin, January 2002	1/24/2002

This ITL Bulletin discusses advances in firewall technology and outlines a number of issues involved in selecting the right kind of firewall for your organizational environment. It contains a series of recommendations for configuring and managing firewalls. The bulletin summarizes NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, which is available for download at http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.

Wack, J., Cutler, K., Pole, J.	Guidelines on Firewalls and Firewall	NIST SP 800-41 (http://csrc.nist.gov/publications/nistpubs/index.html)	1/3/2002

This document provides introductory information about firewalls and firewall policy. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments. It is an update to NIST Special Publication 10, Keeping Your Cite Comfortably Secure: An Introduction To Firewall Technology. This document covers IP filtering with more recently worked policy recommendations, and deals generally with hybrid firewalls that can filter packets and perform application gateway services. This document also contains specific recommendations for policy as well as a simple methodology for

Watson, C.I., Casasent, D.	Fingerprint Matching Using Distortion Tolerant Filters	Advances in Fingerprint Recognition, edited by Nalini Ratha	

The purpose of this paper is to discuss the use of distortion tolerant filters to improve the performance of fingerprint correlation matching. Previous work has shown that correlation matching of fingerprints is susceptible to larger false alarm rates than more traditional minutiae based methods. The elasticity of the finger-print creates enough distortion to produce poor results in correlation matching, be-cause the correlation matcher uses the global ridge structure of the fingerprint image. A way to improve correlation matcher performance is to create filters that combine several elastic distorted versions of the fingerprint images. In this work three different distortion tolerant filters are tested: average, synthetic discriminate function (SDF), and minimum

Westlund, H.B., Meyer, G.W., Hunt, F.Y.	The Role of Rendering in Measurement Science for Optical Reflections	NIST Journal of Research, Vol. 107, No. 3, pp.247-259, May-June	6/1/2002

Rendering is the process of producing a synthetic image using a computer. The best known application is animation and simulation of scenes for the entertainment industry but recognition of its value as a tool for product design in other areas is increasing. Here we report the results of our work to produce visually and radiometrically accurate renderings of selected appearance attributes of sample coated surfaces.

Witzgall, C.J., Cheok, G.S.	Experiences with Point Cloud	Proceedings of the International Society for Automation and Robotics in Construction

The development of LADAR (laser distance and ranging) technology to acquire 3D spatial data made it possible to create 3D models of complex objects. Because an unobstructed line-of-sight is required to capture a point on an object, an individual LADAR scan may acquire only a partial 3D image, and several scans from different vantage points are needed for complete coverage of the object. As a result there is a need for software which registers various scans to a common coordinate frame. NIST is investigating direct optimization as an approach to numerically registering 3D LADAR data without utilizing fiduciary points or matching features. The primary capability is to register a point cloud to a triangulated surface--a “TIN” surface. If a point cloud is to be registered against another point cloud, then the first point cloud is meshed in order to create a triangulated surface against which to register the second point cloud. The direct optimization approach to registration depends on the choice of the measure-of-fit to quantify the extent to which the point cloud differs from the surface in areas of overlap. Two such measures-of-fit have been implemented. Data for an experimental evaluation were collected by scanning a box, and registration

Zhang, N.F., Sedransk, N., Jarrett, D.G.	Statistical Uncertainty Analysis of Key Comparison CCEM-K2	IEEE Transactions on Instrumentation and Measurement

The details of a statistical uncertainty analysis applied to key comparison CCEM-K2 are reported. The analysis presented here provides an approach for addressing known correlations which have been of concern in reporting key comparison results. Uncertainties for each participating national metrology institute (NMI), the key comparison reference value (KCRV), and the pairs of NMIs are determined by fully considering the covariances that interrelate the measurement of the time-dependant transport standards. Uncertainties of the pilot laboratory are treated differently than those of other NMIs due to the predicted values of the transport standards for all NMIs being based on pilot laboratory data. The approach separates the Type A and Type B uncertainty components providing the benefit that data from multiple artifacts (three in this instance) reduces the

Zhang, N.F., Sedransk, N., Jarrett, D.G.	Statistical Uncertainty Analysis of CCEM-K2 Comparisons of Resistance	2002 Conference on Precision Electromagnetic Measurements (CPEM 2002) and IEEE Transactions on Instrumentation

Details of the statistical uncertainty analysis applied to key comparison CCEM-K2 are reported. Formulas were derived to determine the uncertainty of the combined difference between the measurements of multiple artifacts by an NMI and the corresponding predictions based on pilot lab measurements. In addition, the uncertainties of the reference value of the key comparison and the degrees of equivalence between two NMI’s are obtained.