C CE & TECHNOLOGY:

A SURVEY OF REMOTE MONITORING

DEPARTMENT OF COMMERCE * NATIONAL BUREAU OF STANDARDS *

NBS Special Publication 500-42

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, and the Institute for Computer Sciences and Technology.

THE NATIONAL MEASUREMENT LABORATORY provides the national system of physical and chemical and materials measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; conducts materials research leading to improved methods of measurement, standards, and data on the properties of materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government Agencies; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

Absolute Physical Quantities[2] — Radiation Research — Thermodynamics and Molecular Science — Analytical Chemistry — Materials Science.

THE NATIONAL ENGINEERING LABORATORY provides technology and technical services to users in the public and private sectors to address national needs and to solve national problems in the public interest; conducts research in engineering and applied science in support of objectives in these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the utlimate user. The Laboratory consists of the following centers:

Applied Mathematics — Electronics and Electrical Engineering[2] — Mechanical Engineering and Process Technology[2] — Building Technology — Fire Research — Consumer Product Technology — Field Methods.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides scientific and technical services to aid Federal Agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal Agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following divisions:

Systems and Software — Computer Systems Engineering — Information Technology.

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington,D.C. 20234.

[2] Some divisions within the center are located at Boulder, Colorado, 80303.

The National Bureau of Standards was reorganized, effective April 9, 1978.

COMPUTER SCIENCE & TECHNOLOGY:

A Survey of Remote Monitoring

Gary J. Nutt, Ph.D.
Consultant

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary

Jordan J. Baruch, Assistant Secretary for Science and Technology

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Issued January 1979

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-42
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-42, 34 pages (Jan. 1979)
CODEN: XNBSAV

Library of Congress Cataloging in Publication Data

Nutt, Gary J
A survey of remote monitoring.
(Computer science & technology) (National Bureau of Standards special publication ; 500-42)
Supt. of Docs. no.: C13.10:500-42
1. Electronic digital computers--Evaluation. I. Title. II. Series. III. Series: United States. National Bureau of Standards. Special publication ; 500-42.
QC100.U57 no. 500-42 [QA76.9.E94] 602'.1s [621.38] 78-26313

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1978

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
Stock No. 003-003-02013-3 Price $1.50
(Add 25 percent additional for other than U.S. mailing).

TABLE OF CONTENTS

A SURVEY OF REMOTE MONITORING

Abstract

This report describes remote monitoring in the application areas of performance evaluation, diagnostic testing, performance assurance and system security testing. The evolution of remote monitoring is briefly reviewed and, then, remote monitors are categorized into seven classes. Several example systems are discussed for each classification, along with their capabilities in each application area. The views presented in this report represent only those of the author, an independent consultant, and should not be construed as a policy statement of NBS or any other organization.

Key Words:

Diagnostic testing; performance assurance; performance evaluation; remote monitoring; system security testing

NOTE:

Reports on commercial developments included in the publication were obtained from the open literature, supplemented by documentation and correspondence, referenced by permission. Inclusion or exclusion of specific companies, developments, or products cannot be construed as recommendation or endorsement by the National Bureau of Standards.

Paul F. Roth
Systems and Software Division
Institute for Computer
Sciences and Technology

INTRODUCTION

The general area of remote monitoring of computer systems encompasses a broad spectrum of mechanisms for a wide variety of purposes. In this report, the discussion is restricted to monitoring systems or studies where a mechanism is used to measure or observe the performance of a computer system, and that mechanism can be controlled by another device or a human from some geographically distinct location. In most cases, it is expected that the monitoring device itself is designed to collect data about the host system, perform at least preliminary filtering of the raw data, and then either store the filtered data for retrieval by the central controller or immediately transmit the filtered data to the central monitor controller. The nomenclature used for the various constituents, then,is as follows: The *host system* is the installation being monitored; a monitor that is local to the host is referred to as a *remote monitor*. The remote monitor is ultimately controlled from a central site by the *central monitor controller*. The host computer is considered to be the remote facility, while the measurement control and analysis take place at the central site.

This classification of remote monitors admits such approaches as: those implemented purely in software which can be interrogated from an external terminal, programmable hardware monitors, hardware monitors distributed over different portions of the host machine, hybrid monitors, monitors used in distributed computer networks, fault diagnosis monitors, and extended consoles for a computer system. Each of these categories will be discussed in detail in a later section of this report. The classification excludes classic hardware monitors that require plugboard alterations to change the logical combination of probe signals. It also excludes pure software-implemented monitors which use the normal operating system facilities for "triggering," reporting and recording.

Remote monitors are being used in a number of ways that earlier, locally controlled monitors were not used. The most obvious use of the monitors is for gathering performance data. Remote performance monitor facilities are frequently divided into a number of remote data gathering mechanisms plus a single, shared facility to analyze data and prepare reports; the Tesdata facilities are examples of this type.[60] Distributed monitors, perhaps best exemplified by the PARTNER package for Control Data 6000 series machines,[65] are also frequently used for performance measurements; the idea here is to dedicate certain hardware facilities of the host system to the measurement function. Programmable hardware monitors are merely a refinement of earlier hardware monitors, and also are primarily used for performance measurement.

A newer application of remote monitors is for computer system diagnosis and remote exercising of a computer system. A number of computer manufacturers have included this capability in their current product line.[5,32,47,58,59] The basic idea is to replace the conventional operator's console with an intelligent device such as a minicomputer. The intelligent console can be used to inspect any of a number of conditions that

Superscript numbers indicate literature references at end of the report.

exist in the host machine, allowing the observed condition to be analyzed, recorded or transmitted on a telecommunications link to a remote controller. The remote controller may be a human operator or another computer system. Although this is apparently a new concept to most machine manufacturers, it should be noted that Control Data 6000 series computer systems have used this approach to implement their consoles for a number of years.[57]

A new area for which remotely controlled monitors might be employed is that of performance assurance and safeguard studies. The goal is to monitor the workload of a computer system in order to either assure a given level of performance, or to assure that a computer system is not being used for tasks that were not intended to be executed on that system.

Although it would be satisfying to be able to monitor a processor's program counter to determine what program the processor is executing, this is obviously impossible in the general case. It is easy to construct an example that shows that if one could write an algorithm that inspects the program counter locus and identifies a corresponding algorithm, then one ought to be able to write a similar algorithm that inspects the program counter locus and indicates whether the corresponding algorithm will ever terminate or not. The latter algorithm has been proven to be impossible to construct.[19] Nevertheless, there are other activities in the computer system that can be observed with a monitor, e.g. resouce utilization. One can easily compute the ratio of input/output time to central processor time for a given job. This will allow one to partition heavy computer jobs from input/output bound jobs.

Although it is impossible to identify arbitrary programs in execution, it may be possible to recognize a small set of programs when they are executing on the host system. For example, suppose that an installation is intended to only execute programs P_1, P_2... P_n (on arbitrary data). It may be possible to employ heuristic techniques to recognize exactly when one program from that set executes, while any unrecognizable program is declared to be illegal. In this case, remote monitoring techniques can be used to recognize the "signature" of each of the n acceptable programs.

Finally, remote monitors may be used to enhance system security or to provide a mechanism for checking the security of a system. It is clear that the presence of monitors of any type are a threat to the overall security of a computer system, e.g. see references 6 and 13. Whenever a mechanism (i.e. a monitor) is provided the capability of observing critical portions of the operating system, then that same device can be maliciously employed to penetrate the conventional security mechanisms of that system. By partitioning a monitor into a local internal component and a remote external component, system security has a much better chance of being effective. The internal monitor can be written as an internal portion of the operating system itself, subject to the same design constraints (such as proof of correctness, restricted entry points, authorized access, etc.) as other modules. The attendant software is essentially data-gathering code, which is simpler and easier to make secure than a full software monitor. The external portion of the monitor is allowed to access the internal portion through normal, secure paths, thus allowing authorization checks and entries into predefined procedures of the operating system.[40] Although this approach is not totally secure, it offers a much more effective security policy than undisciplined monitoring of the host system.

Another variant of remote monitors can be used to audit a computer system's security state. The basic idea is to distribute a monitor of internal and external components, as above. The external portion is used interactively by a human that is responsible for system security to audit various portions of the machine with the aid of the internal portion of the monitor. This approach is used in the WWMCCS computer systems,[29] and will be discussed at length in the body of this report. The Rand Corporation has also investigated the use of monitors to detect data bank intrusions and to delay the intruder until other protective action can be taken.[53]

In the remainder of this report the background of remote monitoring will first be examined. The evolution of present-day monitoring systems will be traced from early performance monitoring work. The main body of this report is the next section; seven categories of remote monitors are defined, and a number of examples of each category are discussed. The final section draws some conclusions about capabilities and limitations for various application areas and looks briefly at future trends in remote monitoring.

BACKGROUND

In this section of the report, the evolution of remote monitors is discussed beginning with hardware and software monitors of the 1960-1970 era. In the early 1970's monitoring techniques and tools became substantially more sophisticated, leading to the development of mechanisms that could be construed as remote monitors. This section will briefly describe this evolution into current remote monitoring technology.

Computer system monitoring has become a primary component of system design, manufacture, and maintenance because of its application to performance evaluation. Although testing instruments (e.g. oscilloscopes) were frequently used to monitor the hardware at a very low level, system monitoring did not really begin to be needed until the mid 1960's. In the early part of that decade, computer systems began to reach a level of sophistication where resources were shared among a set of users. Once resource sharing was introduced, then resource utilization became an important metric for that system. If utilization was too high, then the resource represented a bottleneck to system progress; if utilization was too low, then the resource was either over-configured or, perhaps, was being prevented from being used effectively by bottlenecks elsewhere in the system. The result was frantic activity in the areas of hardware and software monitor development.