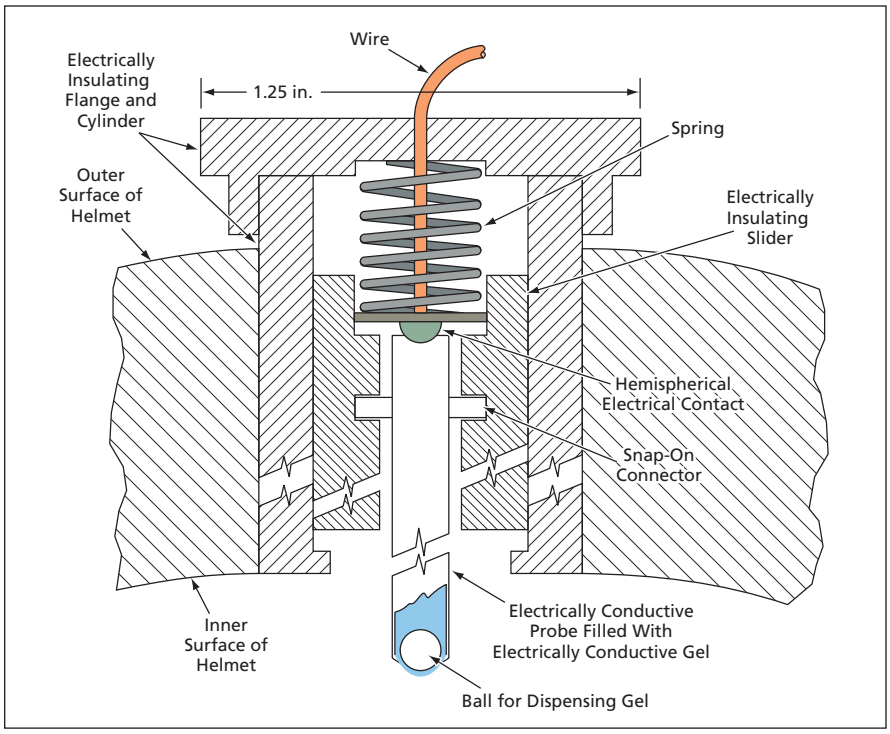
Mobile Collection and Automated Interpretation of EEG Data

Diagnoses could be performed while subjects engaged in ordinary activities.

NASA's Jet Propulsion Laboratory, Pasadena, California

A system that would comprise mobile and stationary electronic hardware and software subsystems has been proposed for collection and automated interpretation of electroencephalographic (EEG) data from subjects in everyday activities in a variety of environments. By enabling collection of EEG data from mobile subjects engaged in ordinary activities (in contradistinction to collection from immobilized subjects in clinical settings), the system would expand the range of options and capabilities for performing diagnoses.

Each subject would be equipped with one of the mobile subsystems, which would include a helmet that would hold "floating electrodes" (see figure) in those positions on the patient's head that are required in classical EEG data-collection techniques. A bundle of wires would couple the EEG signals from the electrodes to a multi-channel transmitter also located in the helmet. Electronic circuitry in the helmet transmitter would digitize the EEG signals and transmit the resulting data via a multidirectional RF patch antenna to a remote location.



This **Probe Assembly** would be one of several mounted in a helmet. Each such assembly would hold an EEG electrode in one of the required positions on the wearer's head.

At the remote location, the subject's EEG data would be processed and stored in a database that would be auto-administered by a newly designed relational database management system (RDBMS). In this RDBMS, in nearly real time, the newly stored data would be subjected to automated interpretation that would involve comparison with other EEG data and concomitant peer-reviewed diagnoses stored in international brain data bases administered by other similar RDBMSs.

This work was done by Frederick Mintz and Philip Moynihan of Caltech for NASA's Jet Propulsion Laboratory. Further information is contained in a TSP (see page 1).

In accordance with Public Law 96-517, the contractor has elected to retain title to this invention. Inquiries concerning rights for its commercial use should be addressed to:

Innovative Technology Assets Management
JPL
Mail Stop 202-233
4800 Oak Grove Drive
Pasadena, CA 91109-8099
(818) 354-2240
E-mail: iaoffice@jpl.nasa.gov

Refer to NPO-42386, volume and number of this NASA Tech Briefs *issue, and the page number.*

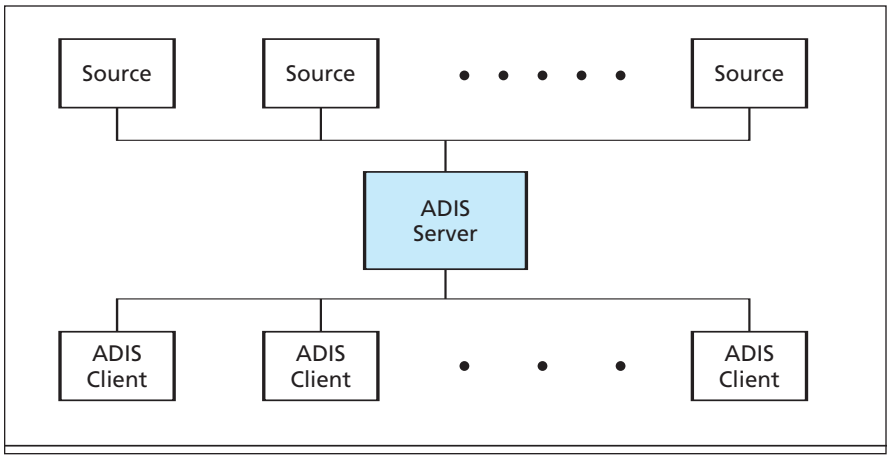
System for Secure Integration of Aviation Data

Data can be analyzed without compromising security or anonymity.

Ames Research Center, Moffett Field, California

The Aviation Data Integration System (ADIS) of Ames Research Center has been established to promote analysis of aviation data by airlines and other interested users for purposes of enhancing the quality (especially safety) of flight operations. The ADIS is a system of computer hardware and software for collecting, integrating, and disseminating aviation data pertaining to flights and specified flight events that involve one or more airline(s). The ADIS is secure in the sense that care is taken to ensure the integrity of sources of collected data and to verify the authorizations of requesters to receive data. Most importantly, the ADIS removes a disincentive to collection and exchange of useful data by providing for automatic removal of information that could be used to identify specific flights and crewmembers. Such information, denoted sensitive information, includes flight data (here signifying data collected by sensors aboard an aircraft during flight), weather data for a specified route on a specified date, date and time, and any other information traceable to a specific flight. The removal of information that could be used to perform such tracing is called "de-identification."

Airlines are often reluctant to keep flight data in identifiable form because



The **ADIS Server** receives aviation data from multiple sources, integrates the data, and provides the integrated data in de-identified forms to authorized (ADIS client) end users.

of concerns about loss of anonymity. Hence, one of the things needed to promote retention and analysis of aviation data is an automated means of de-identification of archived flight data to enable integration of flight data with non-flight aviation data while preserving anonymity. Preferably, such an automated means would enable end users of the data to continue to use pre-existing data-analysis software to identify anomalies in flight data without identifying a specific anomalous flight. It would then also be possible to perform statistical analyses of integrated data.

These needs are satisfied by the ADIS, which enables an end user to request aviation data associated with de-identified flight data. The ADIS includes client software integrated with other software running on flight-operations quality-assurance (FOQA) computers for purposes of analyzing data to study specified types of events or exceedences (departures of flight parameters from normal ranges). In addition to ADIS client software, ADIS includes server hardware and software that provide services to the ADIS clients via the Internet (see figure).

The ADIS server receives and integrates flight and non-flight data pertaining to flights from multiple sources. The server accepts data updates from authorized sources only and responds to requests from authorized users only. In order to satisfy security requirements established by the airlines, (1) an ADIS client must not be accessible from the Internet by an unauthorized user and (2) non-flight data as airport terminal information system (ATIS) and weather data must be displayed without any identifying flight information. ADIS hardware and software architecture as well as encryption and data display scheme are designed to meet these requirements.

When a user requests one or more selected aviation data characteristics associated with an event (e.g., a collision, near miss, equipment malfunction, or exceedence), the ADIS client augments the request with date and time information from encrypted files and submits the augmented request to the server. Once the user's authorization has been verified, the server returns the requested information in de-identified form.

This work was done by Deepak Kulkarni, Yao Wang, Rich Keller, Tom Chidester, and Irving Statler of Ames Research Center; Bob Lynch of Flight Safety Consultants; Hemil Patel and May Windrem of SAIC; Naveen Ashish of USRA-RIACS; and Bob Lawrence of Safe Flight.

This invention is owned by NASA and a patent application has been filed. Inquiries concerning rights for the commercial use of this invention should be addressed to the Ames Technology Partnerships Division at (650) 604-2954. Refer to ARC-15036-1.