INL/EXT-11-23301

Communication Pathways in the Light Water Reactor Sustainability Online Monitoring Project

Nancy J. Lybeck
Magdy S. Tawfik
Binh T. Pham
Vivek Agarwal
Jamie B. Coble

September 2011

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-11-23301

Communication Pathways in the LWRS Online Monitoring Project

Nancy J. Lybeck, Magdy S. Tawfik, Binh T. Pham, Vivek Agarwal
Idaho National Laboratory
Idaho Falls, ID 83415

Jamie Coble
Pacific Northwest National Laboratory
Richland, WA 99352

September 2011

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared under Work Package L-11N060201
Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ABSTRACT

Implementation of online monitoring and prognostics in existing U.S. nuclear power plants will involve coordinating the efforts of national laboratories, utilities, universities, and private companies. Large amounts of operational data, including failure data, are necessary for the development and calibration of diagnostic and prognostic algorithms. The ability to use data from all available resources will provide the most expeditious avenue to implementation of online monitoring in existing nuclear power plants; however, operational plant data are often considered proprietary. Secure methods for transferring and storing data are discussed, along with a potential technology for implementation of online monitoring.

CONTENTS

FIGURES

ACRONYMS

AFS	Asset Fault Signature
EAM	Enterprise Asset Management
EPRI	Electric Power Research Institute
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
NEUP	Nuclear Energy University Programs
NPP	Nuclear Power Plant
ORNL	Oak Ridge National Laboratory
PHM	Prognostic Health Management
PNNL	Pacific Northwest National Laboratory
RAID	Redundant Array of Inexpensive Disks
R-MFT	RepliWeb Managed File Transfer
RUL	Remaining Useful Life
SQL	Structured Query Language
TCP	Transmission Control Protocol
USB	Universal Serial Bus
VM	Virtual Machine

Communication Pathways in the LWRS Online Monitoring Project

1. INTRODUCTION

The implementation of online monitoring and prognostics in existing U.S. nuclear power plants (NPPs) is the ultimate goal of the online monitoring pathway. Successful completion of this goal will involve cooperation between many stakeholders, including Idaho National Laboratory (INL), Pacific Northwest National Laboratory (PNNL), Oak Ridge National Laboratory (ORNL), universities participating in the Nuclear Energy University Programs (NEUP), the Electric Power Research Institute (EPRI), utilities, etc. In particular, data are a vital component of any online monitoring system and must be shared among participants.

Large amounts of high-fidelity operational data covering the full range of operating conditions for both healthy and faulted systems are necessary to develop, validate, and calibrate both diagnostic and prognostic models. Failure data are often difficult to obtain in high-risk environments like NPPs, as critical components are replaced on a conservative time-based approach to prevent failure. Additionally, when component failures do occur, the cause of failure is rarely made public. The ability to use data from all available resources will provide the most expeditious avenue to implementation of online monitoring in existing NPPs.

The report summarizing the findings of the "2010 Light Water Reactor Sustainability (LWRS) Workshop on Online Monitoring Technologies" (Baldwin, Tawfik, and Bond 2010) identifies the proprietary nature of plant data as one of the key barriers to implementation of online monitoring in NPPs. Because of this, data security is a significant issue that must be considered as part of this project. The following sections address security concerns in both data transfer and data storage, and one software suite that can be used to implement online monitoring.

2. DATA TRANSFER

American businesses are becoming increasingly aware of the vulnerabilities introduced by the data transfer process (Christensen 2011). Although sending information via encrypted e-mails is a seemingly simple solution, most corporate e-mail servers have significant limitations on file size. Employees often find risky alternatives, including using personal e-mail, unsecure File Transfer Protocol (FTP), and portable storage media (MeriTalk, Axway 2010). The following sections address three available technologies for transferring plant data in support of online monitoring.

2.1 LWRS Online Monitoring Hub

A collaborative work environment has been established using INL portal technologies to serve as a hub for the LWRS online monitoring community (Lybeck, Tawfik, and Pham 2011). The hub is based on Web Center Interaction, an Oracle Project, and uses role-based security to control access to materials. One of the primary features of the hub is file sharing, which could be used as a way for project participants to share raw data files.

Using the INL portal, projects are established within communities of users with common interests (e.g., the LWRS community). Each individual user within a community can only see the projects to which he/she is granted access. The online monitoring hub currently consists of one project under the LWRS community. Additional projects can be added as necessary, allowing the information shared to be

partitioned by access requirements. Project participants would then bear the responsibility of protecting any data downloaded from the hub.

The hub uses Hypertext Transfer Protocol Secure (HTTPS) encryption for secure data transmission during uploading and downloading. The user may also encrypt files prior to uploading to protect business sensitive information; however, classified documents should never be uploaded.

2.2 Managed File Transfers

The transfer of large amounts of data (e.g., hundreds of data files or one very large file) requires a more sophisticated technology. File Transfer Protocol (FTP) is a standard network protocol that is used to move files between computers via a Transmission Control Protocol (TCP)-based network. Encryption should be used when sending files via FTP, which is not a secure protocol. INL hosts a RepliWeb Managed File Transfer (R-MFT) system, enabling users to securely transfer data from a web browser or a desktop client application. R-MFT supports FTP as well as more secure data transfer protocols; capabilities include secure transfers, encryption, digital signatures and authentication.

2.3 Portable Storage Media

Data can also be transferred by shipping a data storage device to the central repository. This can include Universal Serial Bus (USB) drives, portable hard drives, DVDs, etc. These devices are subject to theft and/or loss, and should be stored in a locked cabinet when not in use. Additionally, the data should be encrypted prior to storage on the device. Once the devices are no longer needed, they should be properly destroyed or returned to the originating source.

3. DATA STORAGE

While the hub is an easy and secure way to implement file sharing, there are some limitations to consider as well. Large amounts of raw data files (typically excel files or text files) can be overwhelming. Each individual researcher (or group of researchers in one location) could spend a lot of time organizing the data into a more usable format, most likely a relational database such as Oracle, SQL Server, or MySQL. These databases offer a number of security options that can be used to control data access.

The following discussion is based on a simple data schematic for the development of online monitoring. Data collected at a NPP are stored in a plant data database. Diagnostic rules (or algorithms) are developed based on the plant data. Prognostic algorithms are developed based on plant data along with any available verified data. The diagnostic rules and prognostic algorithms are stored in separate databases. Security of each database is of interest, as in some applications even simple diagnostic thresholds are considered proprietary (e.g., rotorcraft).

All data, whether stored in files on a server or in a database, require a thoughtful approach to security. Data should be protected from unauthorized access, corruption, and loss. In the following subsections, file- and database-specific security issues are addressed.

3.1 Server File Security

Hardware failure, virus attacks, and malicious access are some of the ways in which data files can be lost from a server. Fortunately, there are many technologies that can be used to prevent these losses. Hardware redundancy can provide increased protection (e.g., a Redundant Array of Inexpensive Disks [RAID] is used to divide and replicate data across multiple disk drives so that a single point of failure will not result in lost data). Anti-virus software should be deployed on the server to prevent loss due to malware. Regular, automated data backup is essential, allowing full recovery from unexpected troubles.

Physical access to the server should be restricted. A firewall (either hardware or software) is used to prevent unauthorized external access to data. Folder-level security can be implemented to prevent access from internal users who do not need access. Data from individual sources can be maintained in separate folders, making the job of assigning and controlling access simpler. Additionally, version control software such as subversion can be used to track individual files over time, so that files that have been altered (whether accidental or intentional) can be readily restored if necessary.

3.2 Database Security

Database access is typically controlled using a user authentication (log-in) process. User permissions to select, insert, update, and delete data from individual tables within a database can be explicitly granted or denied by the database administrator. This provides many options for working with data from different sources. Parallel databases can be used, which restricts each database to one data source. Additionally, parallel tables can be created within a database, using the table-level privileges to segregate users.

Referential integrity is used within a database to document relationships between tables. When referential integrity is disabled, data can easily be entered into the database without the supporting information that provides context. Data without context is unusable data. Hence referential integrity should be enforced within the database.

As with file servers, physical access to the server hosting the database should be restricted. A firewall and anti-virus software should both also be used. The database should be automatically backed up on a daily basis to minimize any data loss due to catastrophic failure.

4. IMPLEMENTATION

Implementation of Prognostic Health Management (PHM) in NPPs will require the use of a prognostics architecture, a software product, or suite of products designed to implement the necessary pieces for a complete implementation of PHM (Lybeck et al. 2011). This discussion will focus on a software suite, developed by Expert Microsystems for the EPRI, consisting of four separate, but complimentary, software programs to support health monitoring of power generation systems. Each of the main programs has been developed to act either as a stand-alone product or in cooperation with other advisors. The software tools are designed as web-based user interfaces, but they can be incorporated into other Enterprise Asset Management (EAM) products, such as IBM's Maximo.

The software suite is designed to perform fault diagnosis and prognosis based on available system data sources. Data sources can include plant data historians, online monitoring, and fleet-wide monitoring programs, operator inspection results, etc. The *Diagnostic Advisor* compares actual plant conditions to the stored fault signatures in the *Asset Fault Signature (AFS) Database* to determine if a fault condition exists and identify likely causes. Plant condition data can also be used by the *Remaining Useful Life (RUL) Advisor* in conjunction with the *RUL Database* to estimate the time of failure for systems or components experiencing a fault based on several available prognostic models. Each of these modules is described briefly in later sections. A schematic of the data flow is shown in Figure **1**.

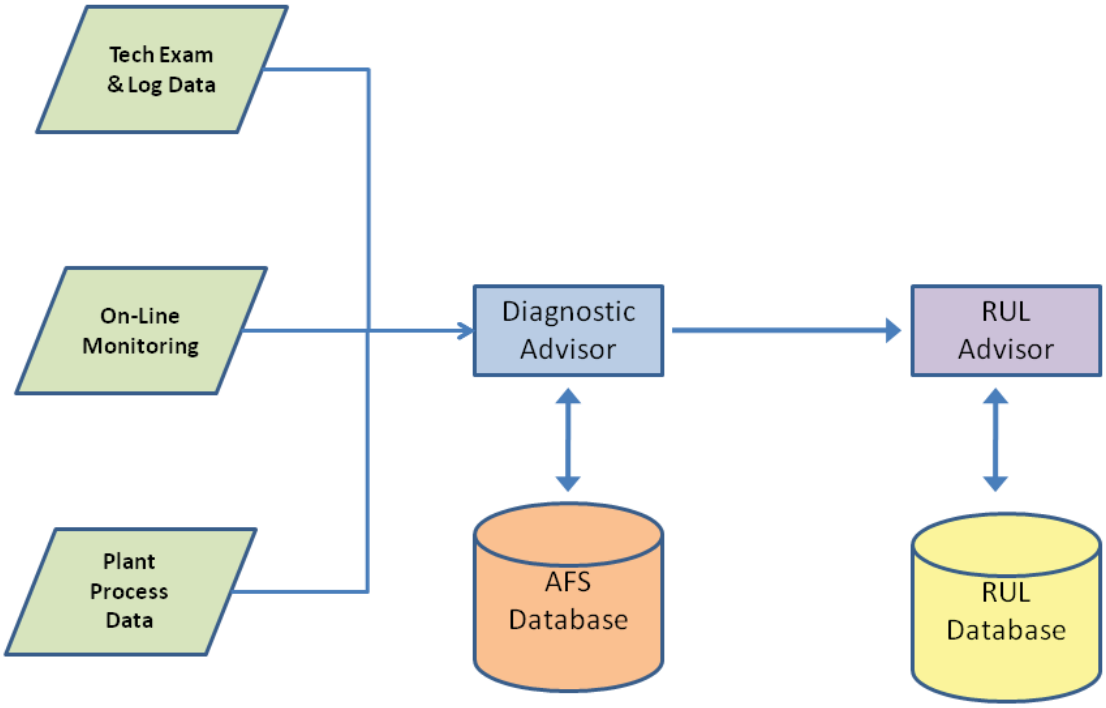

Figure 1. Data flow in the EPRI software suite.

System assets are defined in a five-level hierarchy, from upper- to lower-level: Plant, Unit, System, Equipment, and Component. Fault signatures and prognostic models can be chosen for a specific component, perhaps a bearing in the condensate in the pump for Auxiliary Feed-water System in a NPP, or across the entire population of similar components (in this case, across all bearings). This allows the user to leverage all available information—not only across different utilities, but also across different systems.

Data sources from the plant can be integrated with the EPRI advisors database to allow for system analysis (diagnosis and prognosis), taking into account actual system conditions. These data sources must be linked to specific technologies and state indication routines in *Technical Examinations* (tech exams). Technologies for system assessment are pre-defined, such as vibration, temperature, acoustic noise, etc. These include both continuous-range measurements, such as those collected in online monitoring systems, and categorical measurements, as might result from walk-around inspections (i.e., vibration levels "high," "medium," or "low").

The EPRI products run in Windows XP or later on Internet Explorer Version 7 or later. They also require installation of the Oracle 10g database server. The software is not fully supported by other web browsers or operating systems, but can easily be deployed on a Windows 2008 SP2 32-bit virtual machine (VM).

4.1 AFS Database

The AFS Database is intended to act as a repository to catalog and store asset fault information and retrieve it for use in the Diagnostic Advisor. The AFS Database is designed to serve as an industry-shared repository of fault signatures, allowing EPRI members to leverage the experiences of plants across the entire power generating fleet. Fault signatures define the symptoms seen in online plant data and periodic maintenance inspections, which indicate a specific fault. Fault signatures can be derived from experience,

using the actual plant data and inspection results seen during the fault; Failure Mode and Effects Analysis (FMEA); Failure Mode, Effects, and Criticality Analysis (FMECA); physical models; or subject matter expert opinion.

The database will be expanded based on the experiences and input of participating utilities. Users can define additional fault signatures, based either on experienced faults captured in the Diagnostic Advisor or on theoretical knowledge, for their local AFS database. One example of a fault signature is the higher noise magnitude of a transformer in NPP, which usually indicates reduction in dielectric and thermal strength of insulations (cracks) that leads to higher partial discharge. These additional signatures can be submitted to EPRI for review and fleet-wide release in updates to the system. The database will likely undergo a significant learning period as it is deployed in the fleet, particularly as aging plants experience new age-related fault modes.

4.2 Diagnostic Advisor

The Diagnostic Advisor uses a case-based reasoning approach to diagnose faults based on the available actual system information and the information contained in the AFS database. Diagnosis is performed by retrieving the fault signatures which are most similar to the current symptoms and ranking them according to similarity. The most likely signature is given as the diagnosis, along with alternative, high-ranking possibilities. After the given diagnosis has been reviewed by a subject matter expert, the diagnosis can be either accepted or rejected, and new verified fault signatures can be added to improve the AFS database. This allows the system to learn and improve with each experienced fault.

4.3 RUL Database and Advisor

The RUL Database and Advisor have been released in *Beta* version. One of the goals of the RUL Database is to facilitate industry-wide sharing of RUL information for power plant assets. The Update RUL Signatures process permits a RUL Database Subscriber Utility to export RUL Result history and the known actual (or user-estimated) RUL for the asset type at the end of its service life. The RUL Advisor combines this information with all previously entered "End of Service Condition" records for this asset type. This information is saved for use in verifying and calibrating RUL Models for the Asset Type.

The RUL Advisor has the capability to analyze several disparate prognostic models for a single asset to compare and/or aggregate results. These models can include the predefined models included in the RUL Database, user-defined models based on available plant data, and expert entries of RUL. The plant available information (via tech exams or online monitoring) may lead to reduced uncertainty in the predicted RUL (i.e., narrower prediction bounds on RUL). *Expert Entries* are estimates of RUL provided by a subject matter expert; they are not directly calculated from the available data sources. After individual prognostic models are evaluated, an expert has the opportunity to assign a confidence in each result, called the *Expert Opinion*. This is a discrete ranking of *No Opinion, Strongly Agree, Agree, Disagree,* or *Strongly Disagree*. The advisor assigns a hierarchy to these results, although all RUL estimates are saved and available to the user. RUL results are ranked in the following way (from the RUL Advisor online help):

- The **Expert Entry** will be preferred and reported, if available.
- If more than one entry is available for a model (other than **Expert Entry**), the RUL value for the model scoring with the highest **Expert Opinion** rating will be selected.
- If no model can be selected uniquely based on the highest **Expert Opinion** rating, the model having the lowest reported RUL value will be selected, provided that the model results compared have the same units of measure.

- If none of the above criteria can be determined, the model having the lowest reported RUL value in an absolute numerical sense will be selected for reporting on the Home Screen.

The final decision on the asset RUL relies heavily on expert knowledge, either an expert estimate of RUL or expert opinion of the validity of each prognostic model estimate.

5. SUMMARY

The proprietary nature of operational NPP data presents many challenges to the implementation of online monitoring and prognostics. The presented approach allows the proprietary plant data to be stored separately from the fault signature and remaining useful life databases. The plant may choose which data to share with the fleet-wide database based on individual considerations. This allows better control over access to data from an individual plant, while still achieving the benefits of sharing data from multiple plants. Access to each database can be controlled individually, allowing for a versatile security implementation.

EPRI's suite of tools provides a basis for developing a health monitoring system for power generating plants. More usefully, it provides a repository for sharing diagnostic and prognostic information across the entire fleet of power generating utilities, allowing each member utility to benefit from knowledge derived from the integrated operating history of similar plants, systems, and components. The tools are designed to be flexible enough to use them individually as stand-alone products or together in a full diagnostic and prognostic suite.

6. WORKS CITED

1. Baldwin, T., Tawfik, M., and Bond, L., 2010, "Report from the Light Water Reactor Sustainability Workshop on Online Monitoring Technologies," INL/EXT-10-19500, *June 10–12, 2010, Seattle, Washington*.
2. Christensen, D., 2011, "Information Sharing Wake-Up Call: Customers Now Pushing Organizations to Reconsider How They Transfer Sensitive Files," Retrieved from http://blog.ipswitchft.com/wakeupcall/.
3. Lybeck, N. J., Tawfik, M. S., and Pham, B. T., 2011, "Establishment of a Hub for the Light Water Reactor Sustainability Online Monitoring Community, INL/EXT-11-23080, August 2011,"
4. Lybeck, N., Pham, B., Tawfik, M., Coble, J. B., Meyer, R. M., Ramuhalli, P., et al.. 2011, "Lifecycle Prognostics Architecture for Selected High-Cost Active Components, 2011."
5. MeriTalk, Axway, 2010, "Why Encrypt? Federal File Transfer Report," Retrieved from http://www.meritalk.com/2010-ftpsecurityreport.php.