OSART Good Practices

TECHNICAL SUPPORT

Computer based systems important to safety

Loviisa, Finland

Mission Date; 5-21 Mar., 2007

Usage of portable process simulator for closed loop testing at the supplier's premises.

Simulators are extensively used to support the safe and economical renewal of the automation systems in the plant. In addition to the simulators supporting development, engineering and training, a portable process simulator was also developed. This latter simulator is installed in the laboratory of the manufacturer and connected to the new automation systems important to safety for test purposes. In this test environment a real time closed loop testing is facilitated as a part of the Factory Acceptance Tests. This configuration at the factory supports testing of the safety related systems during normal operational manoeuvres and facilitates testing of the new operational procedures, as well.

Transient tests in the test environment can be also used to prove the dynamic behaviours of the new system, therefore the scope of dynamic system tests on-site can be significantly reduced.

The process simulator has been already used for testing the non safety instrumentation and resulted in several functional findings, which had not been discovered during the open loop.

Tihange, Belgium

Mission Date; 7-23 May, 2007

A single database called THEMIS has been created in order to centralize all information to support the surveillance programme. It contains all the legal requirements (Safety report, ASME, etc), insurance requirements, maintenance requirements including manufacturers' prescriptions, requirements linked to various certificates (ISO, etc) and operating experience. Searches in the database structure can be performed by type of equipment and by type of requirement. All requirements applicable to the equipment concerned can be consulted online. Moreover, a link to Systems Applications and Products (SAP) gives access to the list of periodic tasks performed on specific equipment.

This database is a support tool, which helps to analyzing the requirements related to specific equipment and allows easy access to the highest-level requirement. Software development (material & people) is inexpensive compared to the benefits.

The main benefits are significant time savings for engineers when performing equipment analyses thanks to quick and easy access to relevant data and cost savings due to reduced need to outsource analyses. The database also supports in safety decision-making through automatic access to the most restrictive requirement.

Neckerwestheim, Germany

Mission Date; 8-24 Oct., 2007

Application of a zone model for the security of computer and digital based I&C systems

It is sensible to provide staged protection of computer and digital based I&C systems. The stages take into account the potential risk and threats depending on the system relevance to safety. One practical solution of a graded approach is to divide the computer and digital I&C systems into zones, where graded protection principles can be applied to each zone depending on its relevancy to safety or plant operations. A zone model makes it easier to apply similar protection needs in a complex computer infrastructure and at the same time facilitate the exchange of information in a safe way. The zone model makes it possible to define zone-specific guidelines depending on the protections needs.

At Neckarwestheim Nuclear Power Plant, a zone model to structure the computer and I&C based systems have been implemented together with the necessary and relevant criteria.

The defined computer security zones comprise computers with the same or similar importance concerning safe operation of the plant. Systems belonging to one zone have comparable demands of safeguards. Different computer systems belonging to one zone build a trusted area for internal communication. Zone borders require decoupling mechanisms for data flow in order to prevent un-allowed access or errors to propagate from a zone with lower requirements to a zone with higher demands, for example from the plant IT-system (zone 3) to the process computer (zone 2). Furthermore, demands for physical separation may be applied when defining zone boundaries. This method assures a further deepening of the barrier function and "defense in depth ".
Zones can be partitioned into sub-zones to improve the configuration in order to demarcate one area from another functionally, or to meet different protection needs within one zone.

The zone model easily offers possibility to assign responsibilities to personnel. At the Neckarwestheim NPP responsibility for the security within a zone is allocated to individual department heads. The responsible person manages and organizes all activities concerning computer security within a zone. In addition to that the plant has appointed a computer system security officer (CSSO) who is responsible for the zone model as such. The CSSO documents the zone requirements, advises and supports all those involved and encourages the cross-departmental exchange of information about IT security in general.

Arkansas, USA

Mission Date; 15 Jun.-2 Jul., 2008

Plant Data Server enhances monitoring and trending capabilities.
Site developed software has enabled ANO to maintain consistent high availability and reliability from its plant process computer systems. Developing software on-site has proven very cost effective by maximizing process efficiency and minimizing reliance on and costs paid to vendors.

One of these on-site developed systems is the Plant Data Server (PDS). This computer system enables real-time access of plant data to all plant personnel, including remote access from home. PDS is used to publish data from each unit's Plant Monitoring Computer, along with other data sources, and provides information in a consistent format directly to the desktop. Integrated performance monitoring features (workspaces for customizing trends), links to other performance monitoring documents, enhanced trending tools, tools for easier transient analysis, multi-cycle archives, and a mechanism to annotate plant data events are just a few of the benefits provided by this system.

The data acquisition high level of fidelity allows early identification of very small parameter changes. PDS utilizes an in-house developed data historian that does complete archiving of all data in a high resolution mode. All historical data is available at all times, along with real time data, to facilitate diagnostics of plant problems.

The PDS client is a standard component on the Entergy Nuclear computer desktop and provides a rich set of graphical tools. These tools assist in operations, monitoring transient evolutions, plant maintenance and diagnostics, and performance monitoring. In addition to plant computer data from each unit, PDS also integrates data from the SPDS (Safety Parameter Display System) for each unit, data from the RCP Vibration Monitoring System, WinCDMS (chemistry data), and eSOMS data (operator log readings). Data from any or all of these disparate data sources can be trended together to give plant personnel a powerful data set for analysis.

A notification system is also included in PDS. This enables anyone to be notified by email or pager when any parameter reaches a specified value.

Arkansas, USA

Mission Date; 15 Jun.-2 Jul., 2008

Leveraging wireless technology to enhance plant operations.
A site-wide wireless network (WLAN) has been installed and leveraged to enhance worker effectiveness and productivity at Arkansas Nuclear One.
While wireless networking in itself is not unique, the techniques and extent to which it has been leveraged at ANO is currently at a good level. Also superior to the ANO WLAN implementation is the high standards of reliability and security. The WLAN enables usage of all the benefits gained by networked global applications in areas that were previously without network connectivity; in particular, within the power block of the nuclear unit itself. Once the enabling technology was placed in the hands of very innovative people in line organizations, use of it to bring new solutions to old problems flourished.
Operations, Chemistry & Engineering personnel have leveraged the wireless network in several areas to improve productivity and quality of operations. It provides personnel with real-time plant monitoring for local evolutions, wireless camera monitoring of remote plant areas, and use of a "Pocket PDS" client and other mobility tools on their wireless PDA's.
For Radiation Protection, the wireless network has been the impetus for process productivity and quality enhancement, such as direct entry and update of survey data. Wireless cameras provide quick setup for monitoring high radiation areas; the cameras enable personnel to remain in low dose areas, while monitoring activities.
Maintenance & Outage Management personnel have also leveraged this technology for productivity gains. Wireless VIPER valve actuator testers are used for MOV/AOV testing, and immediate feedback to MOV engineers. Maintenance personnel can access all current reference library material in the field. Also, I&C utilizes wireless PDS in the field to reduce resources needed for string checks.
Management personnel have adopted wireless Tablet PC's as the form factor of choice, and the site-wide wireless network enables them to be in the field while still being constantly connected to online resources and corporate applications.
Security personnel utilize the wireless network in innovative solutions to everyday use, including the Positive Identification System (PIDS) system to photo-verify individuals at access check points, use of ad-hoc local access control at security doors, and wireless pan/tilt/zoom cameras for ad-hoc security monitoring.
Training has also leveraged the wireless network to cut costs and improve the training environment. Trainees have online access to lesson plans, system training manuals, and other classroom reference material.

Oskarshamn, Sweden

Mission Date; 16 Feb.-5 Mar., 2009

Safe and secure computational environment

Core and fuel section uses engineers working within all categories of tasks, including development, validation and production. The same resources sometimes perform tasks within all categories. This poses demands on both the environment of the core calculations and on the resources in order to keep the different tasks apart. Three separate core computational environments have been designed for production, validation and development. These are separated both physically and with firewalls. Except for the three computational environments at client level, three cluster environments have been built in a corresponding manner. A function has also been introduced through which the system administrator can rearrange the computer capacity in the cluster from one environment to another.

The "production environment" has a clean catalogue index and uses only files and software that are validated for production. There is no accessibility to the validation or development environment.

The "validation environment" is a copy of the production environment with the purpose of validating software and codes in an identical environment without tampering with the real production files and inputs. It is only possible to read from the production environment and not write to other environments.

The "development environment" is for programming, developing and testing. It allows for copying of several files or software which is not allowed in the other environments. It is only possible to read from, but not write to other environments.

These three different systems also have different colour schemes and the entire system is handled by a system administrator who also handles the authorization levels of the system giving higher security. An engineer working only with tasks in one environment has no access to other environments resulting in less risk for mixing the system.

The main advantages (compared to the old system) are:
Safety:
- No risk for mixing data, software, inputs and files for different purposes.
- Reduced risk for changing data, inputs and files by mistakes.
- Only validated software and only one version of each software is presented in the production.
- Validation environment allows validating software without influencing production files.
- Since there are only production files when working with production, the catalogue index is clean.

Security:
- The systems are separated physically and with firewalls and there are three different authorization levels.
- System administrator handle accounts, passwords and authorization.
- Limited or no accessibility between the environments.

Seabrook, USA

Mission Date; 6-23 Jun., 2011

Reactor Coolant System (RCS) leak rate management.

Reactor Engineering developed in-house software to automatically calculate and display RCS identified and unidentified leak rates. Key attributes of the automated calculation are:

- No need for operator supplied input data.
- The software accommodates expected operational events such as RCS makeups, Reactor Coolant Drain Tank automatic pump downs, and Volume Control Tank diverts while still maintaining the leak rate calculation.
- Current leak rates are always available to the operators through the station computer.
- Operator set point adjustable computer generated warning alarms are used to detect small changes in leak rate. These operator adjustable leak rate alarms help with timely identification of small increases in leak rates.
- Calculated leak rate values are used directly to monitor compliance with administrative limits on allowed leakage. These administrative limits are set at very low levels (starting with an investigation of leak rate increases in excess of 0.05 gpm) and, when exceeded, call for escalating levels of investigation and monitoring to identify and correct the source of the increased leak rates.
- Computer generated Technical Specification alarms will alert the operator that a condition exceeding a Technical Specification limit has occurred.
- Calculated leak rate values are used directly to by the operators to satisfy Technical Specification surveillance requirements for a periodic RCS inventory balance.
- An on demand computer screen displays the leak rates for the last 72 hours allowing for quick evaluation of near term leak rate trends.
- An RCS leak rate monitoring inoperable alarm if insufficient data exists to allow for a meaningful calculation.

Examples/Results Achieved:
Plant staff are capable of identifying adverse trends in RCS leak rates in a timely manner due to the combination of an automated calculation and associated computer generated alarms. Reactor Engineering also implements the RCS unidentified leak rate monitoring program developed by the PWROG. The purpose of this program is to look for small but statistically significant increases in the RCS unidentified leak rate. In this process a baseline leak rate is determined and action levels are defined if a change in the leak rate is identified. Leak rates normally being monitored are well below the values allowed by Technical Specifications. For example the baseline leak rate in the previous operating cycle was 0.01 gpm. The Technical Specification limit for RCS unidentified leak rate is 1.0 gpm.