Preprint
UCRL-JC-138223

Remote Instrumentation and Safeguards Monitoring for the Star Project

H. M. Buettner, W. Labiak, and A. Spiridon

This article was submitted to International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington, D. C., Nobember 13-17, 2000

June 15, 2000

International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington, DC, November, 2000.

REMOTE INSTRUMENTATION AND SAFEGUARDS MONITORING FOR THE STAR PROJECT

H. Michael Buettner, William Labiak and Alex Spiridon
Lawrence Livermore National Lab
PO Box 808
Livermore, CA 94551
Buettner1@llnl.gov, labiak1@llnl.gov, Spiridon1@llnl.gov,

Keywords: Remote, Monitoring, Neural Nets, Satellite, Encryption

ABSTRACT

A part of the Nuclear Energy Research Initiative (NERI) is the development of the Small Transportable Autonomous Reactor (STAR) for deployment in countries that do not have a nuclear industry. STARs would have an output of from 100 to 150 MW electric, would be fueled in the country of manufacture, and after 15 to 20 years of operation the reactor core would be returned to the country of manufacture for refueling. A candidate STAR design can be found in (Greenspan, 2000). This paper describes the design of the control and monitoring system that might be used. There are two unique features to this system. One is that the monitored information will be transmitted to a remote site for two purposes, safeguards, and allowing experts a great distance away direct access to view the reactor's operating parameters. The second feature is safeguards sensors will be designed into the system and there will monitoring of the safeguards aspects of the system for tampering. Any safeguards anomalies will be sent to the remote site as alarms. Encrypted satellite communications will be used to transmit the data. These features allow the STAR to be operated by a small staff and will reduce the costs of safeguards monitoring by reducing the number of plant visits by inspectors.

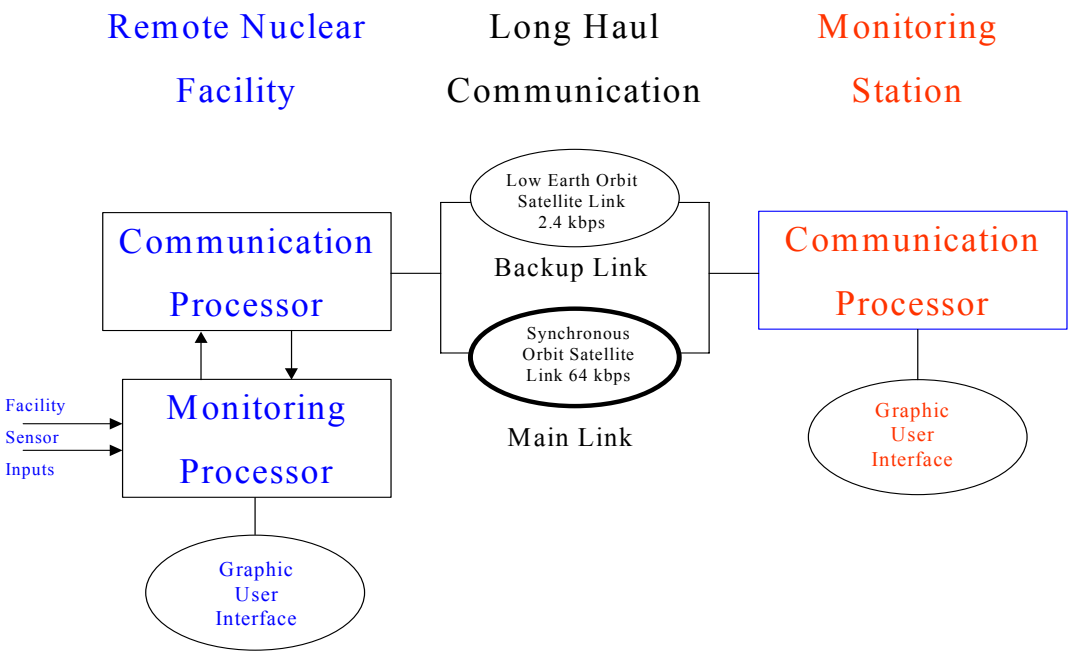
1. INTRODUCTION

The STAR will be installed in countries that do not have a nuclear infrastructure and therefore do not have available a pool of skilled nuclear power scientists and engineers. The STAR is being designed to be simple to operate, however, problems may occur that require expertise that would not be readily available. A remote monitoring capability for the reactor system would solve this problem by bringing key operations information to a remote site where experts could view the data. Even more important is the need for safeguards of the nuclear material. Key operations parameters and security sensors will be remotely monitored and alarms given if it appears that the operation of the reactor, or other activities indicate a potential for diversion of nuclear material. The remote monitoring of safeguards sensors and plant operations together indicate a digital control system design.

The design of the STAR remote monitoring system has several components as shown in Fig. 1. Reactor and security sensor data are acquired at the plant, and transmitted by a secure communications system to a remote monitoring site where the data are received, analyzed, and displayed. Some important aspects of the system design are the integration of security into the system from the sensors back to the remote monitoring station, methods to evaluate sensor performance to detect failure or

tampering, and cost effective, reliable and secure communications between the remote plant and the monitoring station.

Fig. 1 System Overview



2. PLANT AND CONTROL SYSTEM DESIGN

A design basis threat for the plant has not been defined, but the following is assumed. The outsider threat is considered low because the reactor is not designed to be refueled in the field. However, the insider threat is high. A group operating the plant, with concurrence of the electric utility, could shut the plant down and remove the fuel between on-site inspections. The safeguards monitoring portion of the control system would detect a plant shutdown or an unusual operating scenario and report it via the remote system. It is also conceivable that the plant operators would tamper with sensors or spoof them to fool the remote monitoring system. All of these are taken into account in this design.

Starting at the sensor, the data will be transmitted to a data gathering computer system. If the sensor is considered part of the safeguards system, the sensor will have tamper alarm capability installed and will use a line supervision technology to transmit the signal from the sensor to the data gathering computer. There is both a security and cabling advantage if the data can be digitized at the sensor, but this is not required. The data-gathering computer will be a secure computer system located in a secure room with intrusion detection alarms and access control. All operator display information and information for remote monitoring will come from the data gathering computer. This will assure that the data the operators see is the same as the data at the remote site. All operator control commands will pass through the data gathering computer so they may be transmitted to the remote site. Actuation of control commands will either be carried out by the data gathering computer or a separate control system. This part of the design will be determined after a candidate reactor technology is chosen.

The proposed control and monitoring design does require additional infrastructure to implement all of the security features. All accesses to the control system will be recorded for transmission to the remote monitoring site for use in analyzing anomalies. Intrusion detection sensors will also report alarms to the remote site. Redundant computers with dynamic fail-over and backup power supplies will be considered later to balance the design with the redundant long haul communications links. The computer operating system must support very strong security to prevent and detect tampering with the software and files. In particular, the operators must be limited by the computer system to only the controls and displays they need to run the reactor. A failure in some program must not allow the operator access to the computer operating system commands. To protect against software or hardware failures, the reactor system must be self-protecting to fail-safe.

There will be many different types of sensors and data on a STAR. Our design assumes 600 sensor points, and a data rate of 33 BPS each for an overall data rate of 20 KBPS. This number is much lower than a conventional plant, but the STAR is much smaller and simpler. Much of the reactor operations data will be analog which is normally represented in a floating-point format. There will be some purely digital data, which will be represented in an integer format or as a set of bits. Simple security sensor data will also be represented as a set of bits. The design anticipates the need for video images; primarily for assessing alarm conditions and possibly for "live" video. The video for assessments would be digitized, compressed, and recorded in the plant site monitoring system. This video would only be sent when requested by the remote site. A high bandwidth is not required because of the compression, and short duration of one minute before and after an alarm event. Real-time video could also be digitized and compressed, but would require too much bandwidth. If this type of video is used frequently at the remote monitoring site, additional communications bandwidth will be needed. A voice channel will be needed for communications with the operations staff. This channel could be a simple telephone line, or part of the satellite communications system.

Plant data will be scanned and transmitted on a periodic basis to give the remote site a regular snapshot of the state of the plant. The sample rate will be once per second maximum. The remote site will be able to capture and display trends

3.0 COMMUNICATIONS ISSUES

There are three concerns addressed in meeting the communications objectives set for STAR: (1) System and operation cost, (2) Information integrity and error control, and (3) Continuity of monitoring. Properly addressing each of these concerns is important to a viable STAR system.

3.1 System and Operation Costs

The costs can be broken into different categories: initial installation, the running costs, and the cost to develop special system components. It is too early in the design cycle to estimate these costs. However, we can estimate the available revenue from the power generation to bound the costs.

In current dollars one kWh of electric energy sells for $ 0.10. Consider a STAR reactor that generates a 100 megawatts of power, and has a lifetime of 20 years. The revenue from such a reactor is then about $ 3 per second or $ 94.6 M per year, with a total of $ 1.86 billion over the life of the system. This implies the operating costs for communications must be less than a few cents per second. Thus it is reasonable to spend

a few million dollars for the communications equipment and its installation. With the deployment of many STAR reactors, cost sharing will make the economics even more favorable.

3.2 Information Integrity and Error Control

The collection and transmission of reactor data is susceptible to system malfunctions and countermeasures. Threat agents might try to gain access to nuclear fuel and to cover their activity by manipulating the information transmission. Alternatively the threat might be only to disrupt or shut down the operation of the reactor. To protect against these susceptibilities the first priority is to make sure the information received at the monitoring site is actually what is transmitted from the reactor. The transmission system must have an inherently low error, otherwise an accurate status of the whole plant would be difficult to maintain at the remote site.

3.3 Continuity of Monitoring

Control of the bit error rate of data transmission does not by itself prevent the threat of modifying the reactor monitoring data. A time window is opened to modify the reactor monitoring if long transmission delays are allowed, or errors, or link failures, are allowed to occur for a long duration. To control this susceptibility, delay of packet transmission should be allowed only for isolated packets, and not for a continuous long stream of packets. Similarly link errors or disruption should be limited in time. For example, if errors in the transmission link are random and not persistent, it should be possible to use ARQ, Automatic Retransmission Query to correct isolated packets received in error.

4. INFORMATION SYSTEM

A block diagram of the information system is shown in Fig. 1. Satellite links are used to establish two way communications between the remote nuclear reactor and the monitoring station. Most of the traffic will be flowing from the reactor to the monitoring station. The main support link is a duplex 64 KBPS, synchronous orbit satellite dedicated circuit. The back up is a duplex 2.4 KBPS, packet-switched Low Earth Orbit data link. The back up link is used only when the main link goes down. Because of limited capacity and possible longer delays, the back up link provides for spot-checking and trouble shooting only.

4.1 Nuclear Reactor and Remote Monitoring Station

Details of the remote nuclear reactor site are still in the preliminary stages of definition. Data will be collected from a host of information sources. As discussed in section 2, some of the information sources are primarily to maintain the security of the facility; the rest are needed to operate the facility. Under normal operation the collected data are first formatted into packets, and properly encrypted before the error correcting code is added. The scheme can use the TCP/IP/RTP protocol stack to transmit and receive the information. Use of TCP/IP provides compatibility with the interface to the public Internet used by the Low Earth Orbit satellite link. At the anticipated low data bit rate (20 KBPS), all the processing associated with information transmission can be done in a single computer. Processing associated with security and error control at the remote site will be discussed in more detail in section 5.

In the present architecture, each monitoring station is responsible for a single remote nuclear reactor. With a large number of remote nuclear reactors, it will be more

cost effective if one monitoring station supports a number of nuclear reactors. Discussion of such a set up is outside the scope of the present paper, and will not be presented here.

At the monitoring station, the staff can access the data from the remote site with one or more displays. In the back up mode, the data may be compressed before transmission. Under normal operating conditions, the monitoring station acknowledges receipt of the data as part of the process of assuring data integrity. The steps involved in the acknowledgement are described in section 5 on integrity and security and safeguards. The exact form of information exchange to be established in the back up mode is still to be specified.

4.2 Long haul Transmission

The basic information transmission rate is 20000 BPS. In addition to this basic rate there will be overhead for packet protocols, and data encryption. The transmission on the data link will be 30 KBPS including the overhead. With the low error rates expected from the communication link, the Automatic Retransmission Query (ARQ) of packets received in error will introduce little additional load. The impact of transmission delay will have to be considered in the design of the ARQ. Issues of transmission latency will be dealt with in a later study.

The information transmission from the nuclear reactor facilities to the monitoring sites can use the public phone system or satellite communication, since both provide adequate capacity. Selection between the two systems is based on available connectivity, and cost. The discussion in this section is based on the present day status of available communication services, and the findings should be treated with care since the communication industry is changing rapidly. A case in point is the recent withdrawal of the Iridium satellite communication service.

In the present day communication infrastructure, the public phone system is not reliably available to all points in all countries where the nuclear reactors might be deployed. Our design uses satellite communication since it has connectivity to most points in the world. The satellite system could be either Low Earth Orbit (LEO) or Synchronous Orbit (SO), each with its own advantages and limitations. Examples of LEO, are Orbcomm, and Globalstar; and examples of SO system are Intelsat, Skynet, and Columbia. By way of example, Globalstar covers most of the world with notable exceptions of Alaska, central Africa, and North Korea.

SO has the advantage of low operating costs, while the LEO has a low initial installation cost. LEO is targeted at the mobile private user who can not afford a large initial investment and bulky equipment. Here the communication load is sporadic, and low in total volume, so the high running cost will not be an issue.

The SO is the system of choice for the main communication link. The availability of satellite links is better than 99.5%, but not perfect. For example sun flares can affect their performance, and bring down service for short periods (<10minutes) about 8 days a year (Evans, 1999). Thus a backup system is needed.

The LEO is a good choice for a back up link. Its installation cost of few thousand dollars is modest. The operating cost should not be an issue, since the times it will be used are limited to short periods when the main system is down. The back up system will be automatically checked periodically to assure that it is functioning.

5. INTEGRITY AND SECURITY OF COMMUNICATIONS

The integrity and security of the communications system is a primary concern. An overview of the potential susceptibilities and the countermeasures used against them is given in Fig. 2. The communication link suffers errors due to noise or intentional interference. Another form of susceptibility is information warfare. Within this category the attacks are of two types; those which seek to cover the diversion of nuclear fuel to weapon use, and those which seek to bring down the facility monitoring operation. The countermeasures to these susceptibilities are discussed below.

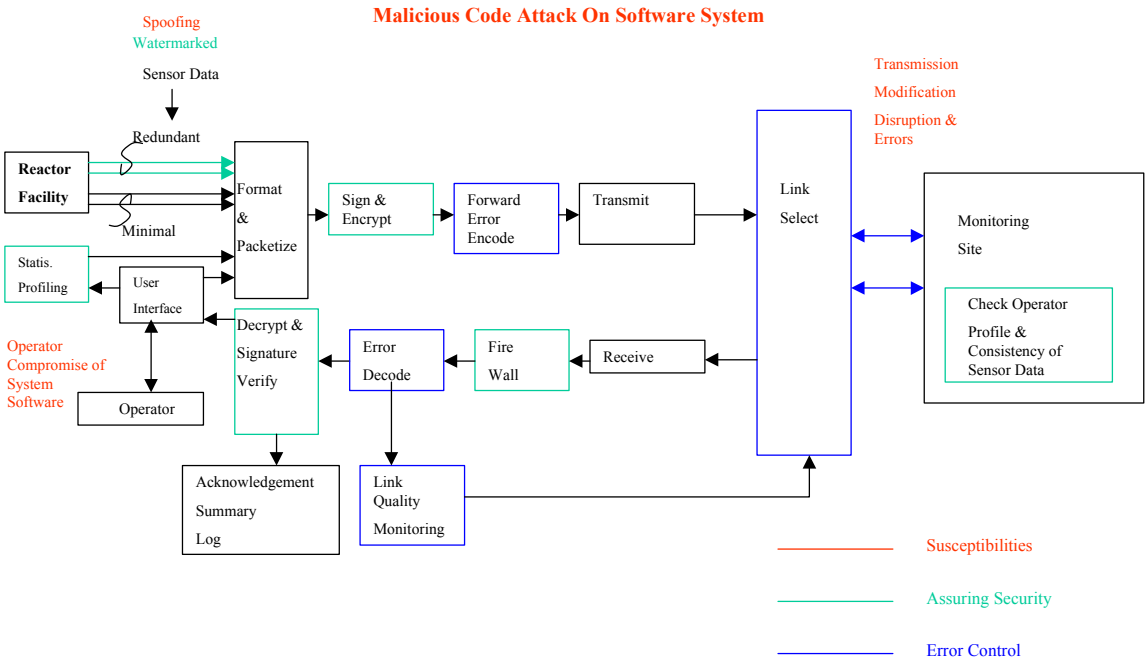


Fig. 2 Susceptibilities of Information Integrity & Counter-countermeasures

5.1 Error Control and Link Availability

The error encoding is done after the encryption and security processing. At the receiving end this requires that error decoding be done first. The decryption processing will implicitly provide some of the error correction. As a minimum, the communication link will have the error control of TCP, which is essentially a parity check sum (Spragins, 1991). This error control is not foolproof, and one undetected packet can be expected per half-hour. The decryption software would detect such an error, requiring a retransmission of the packet.

The link errors are assumed to be isolated in time. The satellite link providers assure link availability at levels on the order of 99.5%. There will be isolated periods of time, on the order of minutes, where the link is down for maintenance or diagnostics. In addition there is always the possibility of satellite terminal equipment failure. To cover these contingencies, there is a need to detect the link failure by monitoring the rate of request for packet retransmission. Once link failure is detected, a switch is made to the back up link.

5.2 Automatic Detection of Sensor Tampering, Failure, and Validation

The sensors in STAR can be protected from tampering by physical security measures. Examples of measures, which fall into this class, are security seals, and placement of sensors in inaccessible or dangerous-to-get-at locations. Such measures have been considered elsewhere and are outside the scope of this paper.

In this paper we are mainly interested in methods which allow for automatic sensor validation for the detection of tampering or failure. There is a large body of work in this area starting in the 1980s. The methods of choice employ artificial neural networks (ANNs), autoassociative neural networks (AANNs), inferential neural networks, artificial neural fuzzy inference systems (ANFIS), and other methods such as statistical process monitoring (SPM) and nonlinear partial least squares systems (NLPLS).

The literature shows a wealth of sensor validation work in the 1990s employing ANNs. When used for signal validation, ANNs have several advantages. Among them are 1) the functional form which relates the process variables is defined by the neural network system, and is by its very nature nonlinear, 2) a properly trained ANN can make predictions in real time, 3) signal estimation using ANNs is less sensitive to measurement noise than direct model-based techniques (Uhrig, 1991), and 4) the non-algorithmic nature of ANNs means that complex systems can be modeled when only system input and output data are available (Reifman, 1997).

Hines et al (1997) have used an ANFIS successfully with data supplied from Florida Power Corporation's Crystal River Unit 3 nuclear power generating station. Using their system, sensor degradation could be detected at levels as low as 0.2% of full-scale range. Their signal validation system can detect a fault or drift in a single channel without affecting the other channels. The system is thus capable of detecting the fault and isolating the channel.

Systems using both AANNs and ANFISs were tested for detecting artificial and actual sensor faults on Crystal River data, and neither method showed overwhelming advantages over the other (Hines et al1997). The main differences between these two system types are 1) AANN sensor estimates contain less noise, and 2) ANFISs are easier and faster to implement and train. ANFIS systems have one major disadvantage, namely that an explosion in the number of inference rules limits the number of possible inputs.

Recent work, not involving AANNs or ANFISs, deserves mention. A SPM sensor validation method based on state variables has been demonstrated for the case of high-temperature short-time milk pasteurization (Negiz and Cinar, 1998). This method can detect and discriminate between sensor drift, bias change or additional noise.

Rasmussen et al (2000) have done recent work employing a nonlinear partial least square (NLPLS) system to perform instrument surveillance and calibration verification (ISCV). An NLPLS system works by replacing the linear regression used in Partial Least Squares (PLS) methods with a single hidden layer ANN, allowing nonlinear relationships to be incorporated into the model. This results in a more accurate model of the process than the standard PLS method with linear regression. This system avoids the pitfalls of setting up and training ANNs, but retains most of the attractive features. Using data from Tennessee Valley Authority's Kingston Unit 9, an ISCV system using NLPLS has been developed for 140 measurement instruments with an average estimation error of less than 1% of the measured value.

5.3 Securing Long Haul Transmission

The sensor data collected at the remote nuclear reactor is signed to authenticate its source, and then encrypted to protect its integrity, and its privacy. The nuclear facility and the monitoring station are each assumed to have their own private key using an RSA public encryption system, with the corresponding public key available to the other end of the communication link. The keys are periodically updated to increase the difficulty of breaking them. Improving the public key system security is critical to assuring a reliable signature and integrity of the data.

5.4 Guarding Against Malicious Code Attack

The software system supporting the transmission of information must be protected from malicious code attacks. Such attacks disrupt the operation of the system and could indirectly allow for the diversion of the nuclear fuel in the period when the system is disrupted. It may also be possible to capture the software for nefarious purposes. For example, it may be possible to capture sensor data before it is secured, store it, and then use the stored sensor data as the source data.

The SO satellite communication link is a dedicated circuit, but it will be interfacing to a standard protocol, and that can open the opportunity for possible malicious code attack. Similarly the LEO might use the public Internet to deliver the packets. Firewalls will be placed at the receiving end of the nuclear facility (and the monitoring station) to restrict the accepted traffic to that transmitted from the nuclear facility address; and the application protocol, to that selected for information exchange.

One other port for malicious code attack is through the user interface. The user should be restricted in the latitude of operation allowed. In addition to normal security guards, such as the use of passwords, monitoring of the user activity will be instituted, and a statistical profile of this activity will be extracted and reported to the monitoring station.

6.0 CONCLUSIONS

We have discussed the remote control system issues relating to STAR and proposed a conceptual design to address them. The final implementation of the design, and parameters specifying it are still to be defined. Remaining issues to be explored are: 1) the specifics of the interface to the satellite system, 2) the cost effectiveness and feasibility of a modular design for the interfaces that allows the use of the less expensive public phone lines (when available) instead of satellites, and 3) the benefit of a custom developed terminal for the STAR application, as opposed to the use of off-the-shelf components.

REFERENCES

Greenspan, E., Shimada, H., Carelli, M.D., Conway, L., Wade, D.C., Brown, N.W., Hossain, Q., 2000. The encapsulated nuclear heat source reactor concept. Proceedings of ICONE 8, Baltimore, MD

Evans, B.G., 1999. *Satellite Communication Systems 3rd edition,* Institute of Electrical Engineers, London, United Kingdom, p. 100.

Spragins, J.D., Hammond, J.L., Pawlikowski, K., 1991. *Telecommunications Protocols and Design,* Addison-Wesley Publishing Company, Reading Mass, p. 553.

Uhrig, R.E., 1991. Potential application of neural networks to the operation of nuclear power plants. *Nucl. Safety*, 32, 68-79.

Reifman, J., 1997. Survey of artificial intelligence methods for detection and identification of component faults in nuclear power plants. *Nucl. Technology*, 119, 76-97.

Hines, J.W., Wrest, D.J., Uhrig, R.E., 1997. Signal validation using an adaptive fuzzy inference system. *Nucl. Technology*, 119, 181-193.

Negiz, A., Cinar, A., 1998. Monitoring of multivariable dynamic processes and sensor auditing. *J. Proc. Cont.*, Nos. 5-6, 375-380.

Rasmussen, B., Hines, J.W., Uhrig, R.E., 2000. Nonlinear partial least squares modeling for instrument surveillance and calibration verification. MARCOM-2000, Knoxville, TN.

This work was performed under the auspices of the U.S. Department of Energy by University of California Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.